Tech Tip
Alteon

SYN Attack Detection

Contents

Contents 1
Overview 1
Sample configuration 5
- Setup 5
- Configuring PC 5
- Configuring Server 6
- Configuring Alteon 7
  - Configuring interfaces 7
  - Configuring real server 9
  - Creating a real servers group 11
  - Configuring virtual IP 12
  - Enabling Client/Server processing 13
  - Enabling Server Load Balancing globally 14
  - Configuring SYN attack parameters 15
- Testing the configuration 16
  - Sending alerts to a remote syslog server 21
    - Configuring syslog on Alteon 21
    - Enabling syslog on the Linux machine acting as a Syslog Server 22

Appendix. Alteon configuration file 24

Overview

One of the most common types of attacks against systems in the internet is a Denial of Service (DoS) attack. The majority of DoS attacks are TCP SYN flooding attacks.

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Usually when TCP connection is to be established Client sends a SYN (synchronization) request to the Server (Figure 1). A SYN request is a TCP packet with a SYN bit set in the TCP header, which lets the receiver know that the sender wants to establish a TCP-based connection. Server process a SYN request, allocates the necessary resources and responds with a SYN ACK (acknowledgement) to acknowledge the receipt of an initial SYN request. At this point connection is at a half-opened state. Client receives a SYN ACK and confirms it with ACK. Thus a three way handshake is complete, TCP connection is opened and Client and Server are ready for communication.

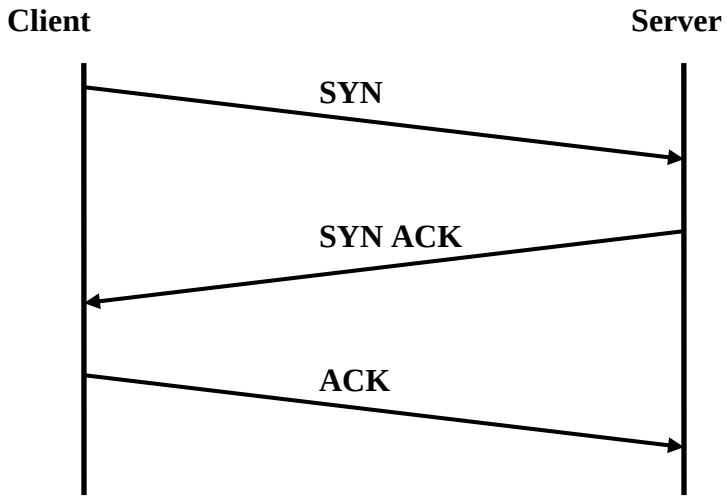


Figure 1

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

In a TCP SYN flooding attack the attacker sends many TCP SYN messages with a forged IP addresses (Figure 2). Server replies to a SYN with a SYN ACK, but attacker never acknowledges these messages, therefore leaving plenty of half-opened connections. The attacker continues to send SYN messages until the Server reaches its half-open connections limit and cannot respond to any new connection requests, thus denying service to clients.

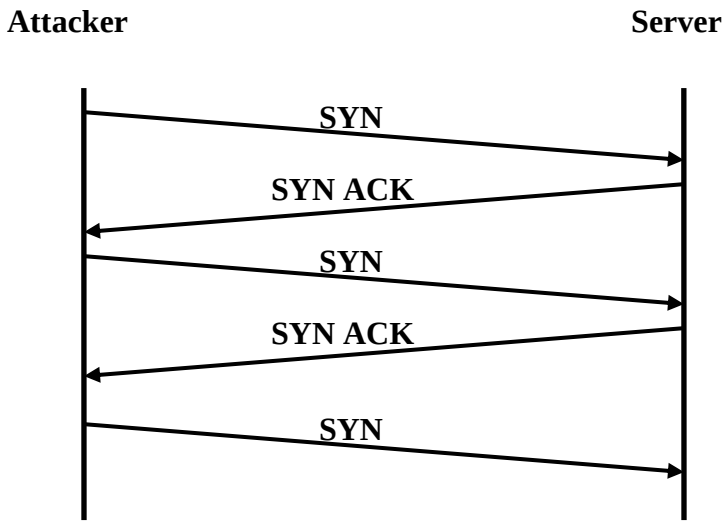


Figure 2

Alteon switch could be used to prevent DoS attacks against the real servers. Alteon's SYN attack detection is enabled automatically when delayed binding feature is enabled.

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

With delayed binding enabled, Alteon intercepts the SYN request before it reaches the real server (Figure 3). Upon receiving a SYN Alteon responds to the Client with a SYN ACK, and waits for the client to return ACK. Once ACK has been received a three way handshake is complete and Client sends a data request. Alteon allocates a session for the connection and starts negotiations with a real Server on behalf of a Client. Once TCP has been negotiated with a real Server, Alteon splices the connection to the Client. Thus two independent TCP connections exist, one between the Client and Alteon and one between the Alteon and a real server.

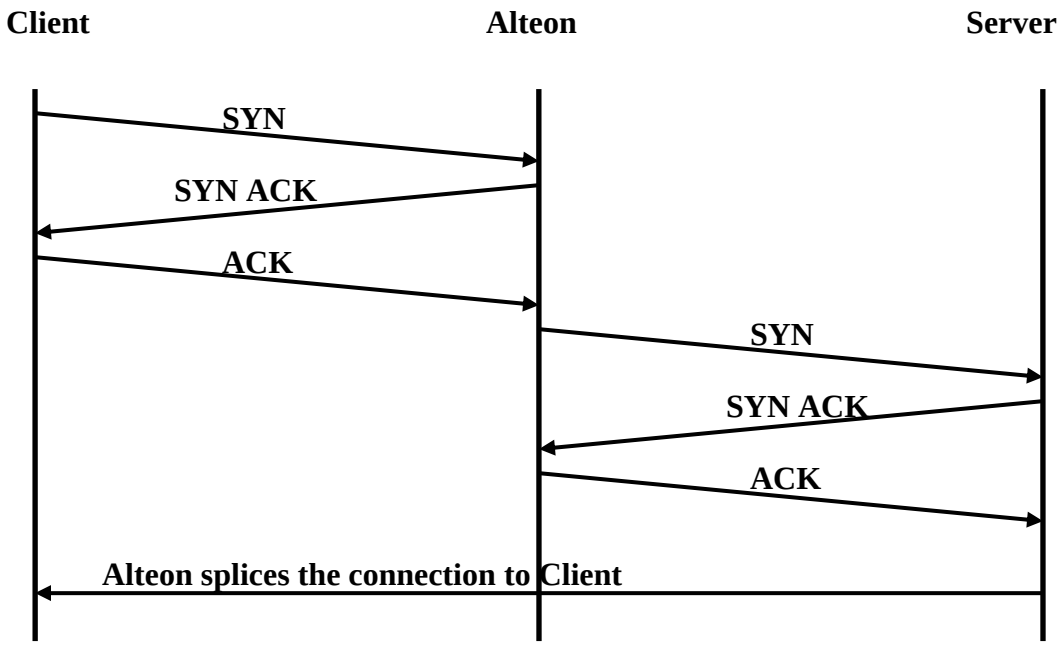


Figure 3

With Alteon switch being between a Client and a Server all TCP connection negotiations go through the Alteon fist. When SYN attack is initiated against the server, Alteon will get the SYN, send the SYN ACK and wait for the ACK from the client. Unlike server Alteon will not associate a session with a half opened connection and resource of both Server and Alteon will not be consumed by SYN requests and legible connections would still be processed.

Alteon's SYN attack detection allows to:

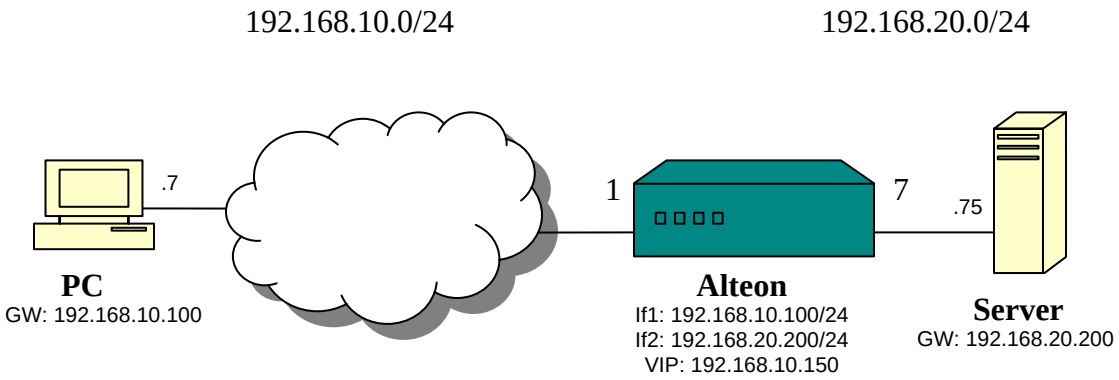
- Track half open connections
- Activate a trap notifying that the configured threshold is exceeded
- Monitor DoS attacks and proactively signal alarm
- Provide enhanced security
- Improve visibility and protection for DoS attacks

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Sample configuration

Setup



PC – Windows 2000 workstation, IP 192.168.10.7/24;
Alteon - Alteon WebOS switch AD3, interface 1 IP 192.168.10.100/24, interface 2 IP 192.168.20.200/24, VIP 192.168.10.150;
Server – Linux RedHat 7.3 with Apache server and syslogd packages installed, IP 192.168.20.75/24.

Configuring PC

Configure IP address (192.168.10.7/24) on PC and set Alteon's interface 1 IP address (192.168.10.100) as a default gateway:

```
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.7
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.100
```

The Packetyzer packet analyzer software (http://www.networkchemistry.com/products/packetyzer) will be used in this example to send SYN requests to the Server.

Download and install the software on PC.

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Configuring Server

Root privileges are required to configure WEB server.

```
[user@linux7 user]$ su
Password:
[root@linux7 user]#
```

Configure IP address (192.168.20.75/24) on Linux machine to be used as a WEB server:

```
[root@linux7 user]# /sbin/ifconfig eth0 192.168.20.75 netmask
255.255.255.0
```

Verify interface is configured correctly:

```
[root@linux7 user]# /sbin/ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:4D:F9:8C
          inet addr:192.168.20.75  Bcast:192.168.20.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:192073 errors:0 dropped:0 overruns:0 frame:0
          TX packets:153176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:11586184 (11.0 Mb)  TX bytes:11552234 (11.0 Mb)
          Interrupt:10 Base address:0x10e0
```

Configure a static route to redirect traffic for 192.168.10.0 network to Alteon's interface 2 (192.168.20.200):

```
[root@linux7 user]# /sbin/route add -net 192.168.10.0/24 gw
192.168.20.200
```

Verify the routing table:

```
[root@linux7 user]# netstat -nr
Kernel IP routing table
Destination  Gateway         Genmask         Flags  MSS Window  irtt Iface
192.168.20.0 0.0.0.0         255.255.255.0   U       40 0          0 eth0
192.168.10.0 192.168.20.200 255.255.255.0   UG      40 0          0 eth0
127.0.0.0    0.0.0.0         255.0.0.0       U       40 0          0 lo
```

This configuration assumes that httpd and apache packages have been successfully installed on Linux machine.
Start the httpd daemon:

```
[root@linux7 user]# /etc/init.d/httpd start
Starting httpd:                                            [  OK  ]
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Configuring Alteon

Note, this sample configuration is started from factory default settings.
Login to the switch. The default admin credentials were used in this example.

```
Enter password:
System Information at 11:05:11 Wed Apr 21, 2004
Alteon AD3
sysName:
sysLocation:
. . .
```

Select **n** to not run the setup script:

```
The switch is booted with factory default configuration.
  To ease the configuration of the switch, a "Set Up" facility which
  will prompt you with those configuration items that are essential
  to the operation of the switch is provided.
Would you like to run "Set Up" to configure the switch? [y/n] n
```

Configuring interfaces

Configure Interface 1.
Enter interface 1 configuration menu:

```
>> Main# /cfg/ip/if 1
------------------------------------------------------------
[IP Interface 1 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Set mask (255.255.255.0), address (192.168.10.100) and enable the interface.

Note: If address is specified before the mask, a broadcast address must be entered using **broad** command.

```
>> IP Interface 1# mask 255.255.255.0/addr 192.168.10.100/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.10.100
Pending new broadcast address:  192.168.10.255
Current status: disabled
New status:     enabled
```

Enter interface 2 configuration menu:

```
>> IP Interface 1# /cfg/ip/if 2
------------------------------------------------------------
[IP Interface 2 Menu]
      addr    - Set IP address
      mask    - Set subnet mask
      broad   - Set broadcast address
      vlan    - Set VLAN number
      relay   - Enable/disable BOOTP relay
      ena     - Enable IP interface
      dis     - Disable IP interface
      del     - Delete IP interface
      cur     - Display current interface configuration
```

Set the mask (255.255.255.0) and address (192.168.20.200) for the interface.
Enable the interface:

```
>> IP Interface 2# mask 255.255.255.0/addr 192.168.20.200/ena
Current subnet mask:     0.0.0.0
New pending subnet mask: 255.255.255.0
Current IP address:     0.0.0.0
New pending IP address: 192.168.20.200
Pending new broadcast address:  192.168.20.255
Current status: disabled
New status:     enabled
```

Disable spanning tree protocol:

```
>> Main# cfg/stp 1/off
Current Spanning Tree 1 setting: ON
New Spanning Tree 1 setting:     OFF
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Apply and save the changes:

```
>> IP Interface 2# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
Switch is currently set to use factory default config block on next
boot.
Do you want to change that to the active config block? [y/n] y
Next boot will use active config block.
```

Verify connectivity to WEB server (192.168.20.75) by pinging it:

```
>> IP Interface 2# ping 192.168.20.75
[host 192.168.20.75, max tries 5, delay 1000 msec]
192.168.20.75: #1 ok, RTT 0 msec.
192.168.20.75: #2 ok, RTT 1 msec.
192.168.20.75: #3 ok, RTT 1 msec.
192.168.20.75: #4 ok, RTT 1 msec.
192.168.20.75: #5 ok, RTT 1 msec.
Ping finished.
```

Verify connectivity to PC (192.168.10.7):

```
>> IP Interface 2# ping 192.168.10.7
[host 192.168.10.7, max tries 5, delay 1000 msec]
192.168.10.7: #1 ok, RTT 0 msec.
192.168.10.7: #2 ok, RTT 1 msec.
192.168.10.7: #3 ok, RTT 1 msec.
192.168.10.7: #4 ok, RTT 1 msec.
192.168.10.7: #5 ok, RTT 1 msec.
Ping finished.
```

Configuring real server

Configure real server on Alteon.
Enter real server configuration menu for the real server 1:

```
>> Main# /cfg/slb/real 1
------------------------------------------------------------
[Real server 1  Menu]
      layer7  - Layer 7 Command Menu
      rip     - Set IP addr of real server
      name    - Set server name
      weight  - Set server weight
      maxcon  - Set maximum number of connections
      tmout   - Set minutes inactive connection remains open
      backup  - Set backup real server
      inter   - Set interval between health checks
      retry   - Set number of failed attempts to declare server DOWN
      restr   - Set number of successful attempts to declare server UP
      addport - Add real port to server
      remport - Remove real port from server
      remote  - Enable/disable remote site operation
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

```
      proxy   - Enable/disable client proxy operation
      submac  - Enable/disable source MAC address substitution
      ena     - Enable real server
      dis     - Disable real server
      del     - Delete real server
      cur     - Display current real server configuration
```

Set real IP (192.168.20.75) for the real WEB server:

```
>> Real server 1 # rip 192.168.20.75
Current real server IP address:     0.0.0.0
New pending real server IP address: 192.168.20.75
```

Enable real server 1:

```
>> Real server 1 # ena
Current status: disabled
New status:     enabled
```

Apply and save the changes:

```
>> Real server 2 # apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Creating a real servers group

Add real servers to a group.

Create a group 1 on the Alteon and enter group configuration mode:

```
>> Main # /cfg/slb/group 1
------------------------------------------------------------
[Real server group 1 Menu]
      metric  - Set metric used to select next server in group
      content - Set health check content
      health  - Set health check type
      backup  - Set backup real server or group
      name    - Set real server group name
      realthr - Set real server failure threshold
      viphlth - Enable/disable VIP health checking in DSR mode
      add     - Add real server
      rem     - Remove real server
      del     - Delete real server group
      cur     - Display current group configuration
```

Add real server 1 to a group:

```
>> Real server group 1# add 1
Real server 1 added to real server group 1
```

Apply and save the changes:

```
>> Real server group 1# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Configuring virtual IP

Configure the virtual IP for the clients to send requests for the service to.
Enter virtual interface 1 configuration mode:

```
>> Real server group 1# /cfg/slb/virt 1
------------------------------------------------------------
[Virtual Server 1 Menu]
      service - Virtual Service Menu
      vip     - Set IP addr of virtual server
      dname   - Set domain name of virtual server
      layr3   - Enable/disable layer 3 only balancing
      ena     - Enable virtual server
      dis     - Disable virtual server
      del     - Delete virtual server
      cur     - Display current virtual configuration
```

Set the virtual IP address (192.168.10.150) for the virtual interface:

```
>> Virtual Server 1# vip 192.168.10.150
Current virtual server IP address:     0.0.0.0
New pending virtual server IP address: 192.168.10.150
```

Enable the virtual interface:

```
>> Virtual Server 1# ena
Current status: disabled
New status:     enabled
```

Assign a service (http, or 80) to the virtual interface:

```
>> Virtual Server 1# /cfg/slb/virt 1/service http
[Virtual Server 1 http Service Menu]
      group   - Set real server group number
      rport   - Set real port
      hname   - Set hostname
      httpslb - Set HTTP SLB processing
      pbind   - Set persistent binding type
      rcount  - Set multi response count
      dbind   - Enable/disable delayed binding
      udp     - Enable/disable UDP balancing
      frag    - Enable/disable remapping UDP server fragments
      nonat   - Enable/disable only substituting MAC addresses
      dnsslb  - Enable/disable DNS query load balancing
      ftpp    - Enable/disable FTP SLB parsing for virtual server
      del     - Delete virtual service
      cur     - Display current virtual service configuration
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Set the real server group (group 1) to be associated with the service on virtual interface:

```
>> Virtual Server 1 http Service# group 1
Current real server group:     1
New pending real server group: 1
```

Apply and save the changes:

```
>> Virtual Server 1 http Service# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Enabling Client/Server processing

Enable Client port processing.
Enter the SLB port 1 configuration menu:

```
>> Main # /cfg/slb/port 1
------------------------------------------------------------
[SLB port 1 Menu]
      client  - Enable/disable client processing
      server  - Enable/disable server processing
      rts     - Enable/disable RTS processing
      hotstan - Enable/disable hot-standby processing
      intersw - Enable/disable inter-switch processing
      proxy   - Enable/disable use of PIP for ingress traffic
      pip     - Set Proxy IP address for port
      filt    - Enable/disable filtering
      add     - Add filter to port
      rem     - Remove filter from port
      idslb   - Enable/disable intrusion detection server load balancing
      cur     - Display current port configuration
```

Enable Client processing on port:

```
>> SLB port 1# client e
Current client processing: disabled
New client processing:     enabled
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Enter SLB port 7 configuration menu:

```
>> SLB port 1# /cfg/slb/port 7
------------------------------------------------------------
[SLB port 7 Menu]
      client  - Enable/disable client processing
      server  - Enable/disable server processing
      rts     - Enable/disable RTS processing
      hotstan - Enable/disable hot-standby processing
      intersw - Enable/disable inter-switch processing
      proxy   - Enable/disable use of PIP for ingress traffic
      pip     - Set Proxy IP address for port
      filt    - Enable/disable filtering
      add     - Add filter to port
      rem     - Remove filter from port
      idslb   - Enable/disable intrusion detection server load balancing
      cur     - Display current port configuration
```

Enable Server processing on the port:

```
>> SLB port 7# server e
Current server processing: disabled
New server processing:     enabled
```

Enabling Server Load Balancing globally

Enable server load balancing (SLB) globally:

```
>> Spanning Tree Group 1# /cfg/slb/on
Current status: OFF
New status:     ON
```

Apply and save the changes:

```
>> Layer 4# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]:y
New config successfully saved to FLASH.
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Configuring SYN attack parameters

Enable direct access mode (DAM):

```
>> Configuration# /cfg/slb/adv/direct e
Current Direct Access Mode: disabled
New Direct Access Mode:     enabled
```

Enable delayed binding for virtual interface:

```
>> Configuration# /cfg/slb/virt 1/service http/dbind e
Current delayed binding: disabled
New delayed binding:     enabled
```

Configure SYN attack parameters.
Enter the SLB advanced configuration menu:

```
>> Virtual Server 1 http Service# /cfg/slb/adv
------------------------------------------------------------
[Layer 4 Advanced Menu]
      script  - Scriptable Health Check Menu
      aphttp  - Enable/disable Allow HTTP Health Check on any port
      synatk  - SYN Attack Detection Menu
      ldapver - LDAP version
      imask   - Set virtual and real IP address mask
      mnet    - Set managment network
      mmask   - Set management subnet mask
      pmask   - Set persistent mask
      secret  - Set RADIUS secret
      submac  - Enable/Disable Source MAC Address substitution
      minter  - Set interval of response and bandwidth metric updates
      idslb   - Set real server group number for IDSLB
      pgarp   - Enable/disable Proxy Ip Gratuitous ARP
      dsfail  - Enable/disable Delete Sessions on Service Failure
      direct  - Enable/disable Direct Access Mode
      grace   - Enable/disable graceful real server failure
      matrix  - Enable/disable Virtual Matrix Architecture
      tpcp    - Enable/disable Transparent Proxy Cache Protocol
      fastage - Session table fast-age (1 sec) period bit shift
      slowage - Session table slow-age (2 min) period bit shift
      cur     - Display current Layer 4 advanced configuration
```

Enter SYN attack detection menu:

```
>> Layer 4 Advanced# synatk
------------------------------------------------------------
[SYN Attack Detection Menu]
      intrval - Set SYN attack detection interval
      thrshld - Set SYN attack alarm threshold
      cur     - Display current SYN attack detection configuration
```

Set the SYN attack threshold to, for example, 3. Note, it's a very small number and is used only for testing the SYN attack detection. In the real life setups the threshold is usually set much higher to allow for larger volumes of traffic, threshold is set to 1000 half-opened connections per second by default.

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

```
>> SYN Attack Detection# thrshld 3
Current SYN attack alarm threshold:     1000
New pending SYN attack alarm threshold: 3
```

Apply and save the changes:

```
>> SYN Attack Detection# apply/save
------------------------------------------------------------------
Apply complete; don't forget to "save" updated configuration.
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Testing the configuration

Check the status of SLB:

```
>> Configuration# /info/slb/dump
Real server state:
  1: 192.168.20.75, 00:0c:29:4d:f9:8c, vlan 1, port 7, health 4, up

Virtual server state:
  1: 192.168.10.150,  00:60:cf:46:53:6e
    virtual ports:
    http: rport http, group 1, backup none, dbind
        real servers:
          1: 192.168.20.75, backup none, 1 ms, up

Redirect filter state:

Port state:
  1: 0.0.0.0, client
  2: 0.0.0.0
  3: 0.0.0.0
  4: 0.0.0.0
  5: 0.0.0.0
  6: 0.0.0.0
  7: 0.0.0.0, server
  8: 0.0.0.0
  9: 0.0.0.0
```

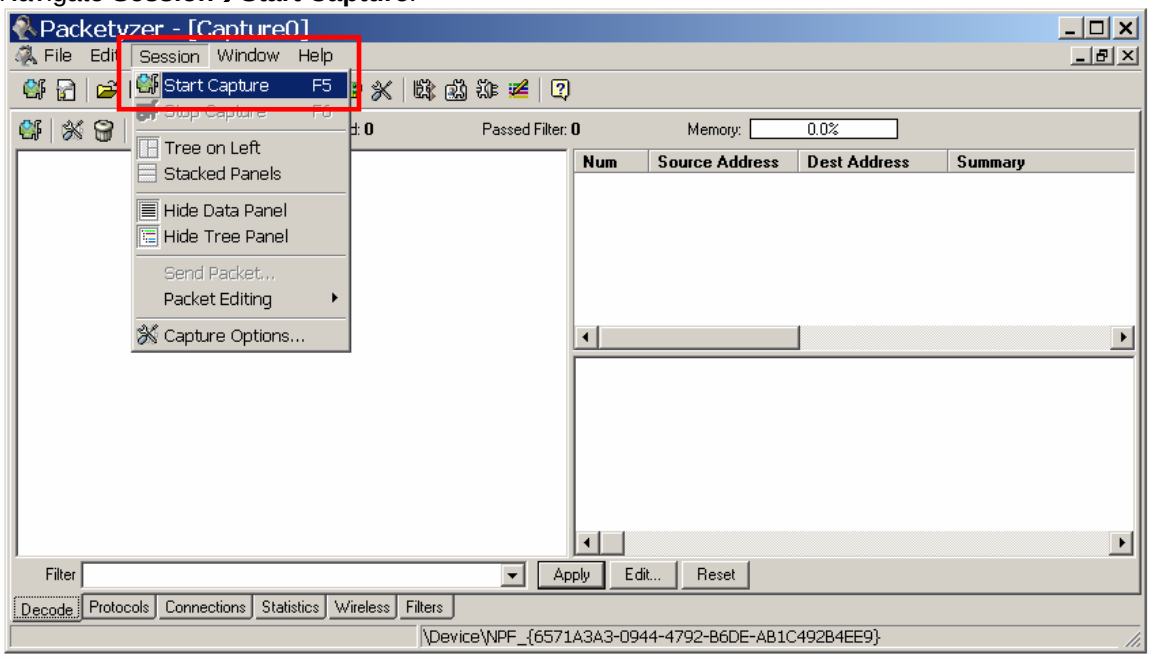
 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

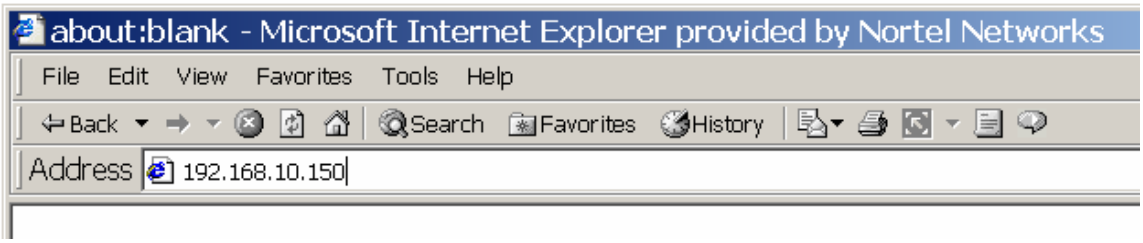
Launch the Packetyzer software from the PC by double clicking on Packetyzer icon:



The **Packetyzer** window appears.
Navigate **Session→Start Capture**:



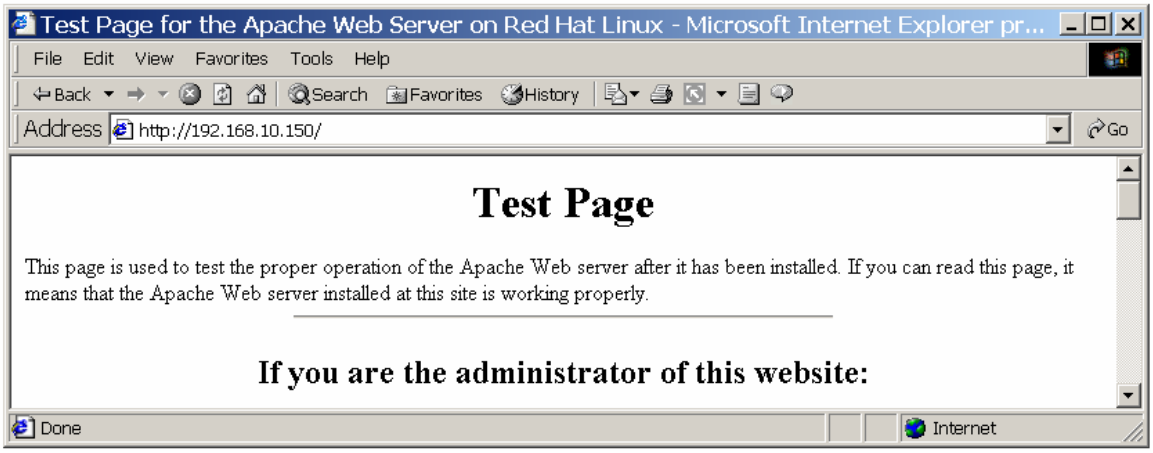
The capture starts.
Open a web browser (Internet explorer in this example) and enter the IP of the virtual server (192.168.10.150):



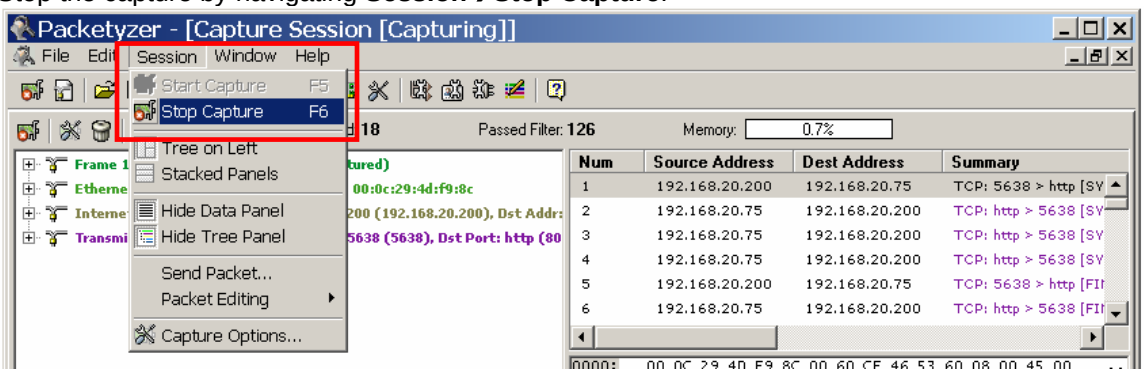
 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

The apache web server test page appears:



Stop the capture by navigating **Session→Stop Capture**:



Clear SLB statistics on Alteon:

```
>> Layer 7 Statistics# /stats/slb/clear
Confirm clearing all SLB statistics [y/n]: y
```

Check SLB statistics:

```
>> Server Load Balancing Operations# /stat/slb/layer7/maint
------------------------------------------------------------------
Layer 7 maintenance stats:
Clients reset by switch on client side:            0
Clients reset by switch on server side:            0
Connection Splicing to support HTTP/1.1:           0
Aged delayed binding sessions:                     0
Half open connections:                             0
Switch retries:                                    0
Random early drops:                                0
Requests exceeded 9000 bytes:                      0
Invalid 3-way handshakes:                          0
Current SP memory units:     1344
Current SEQ buffer entries:     0    Highest:                    0
Current Data buffer use:        0    Highest:                    0
Current SP buffer entries:      0    Highest:                    0
```

 ©2005 Nortel Networks. All Rights Reserved

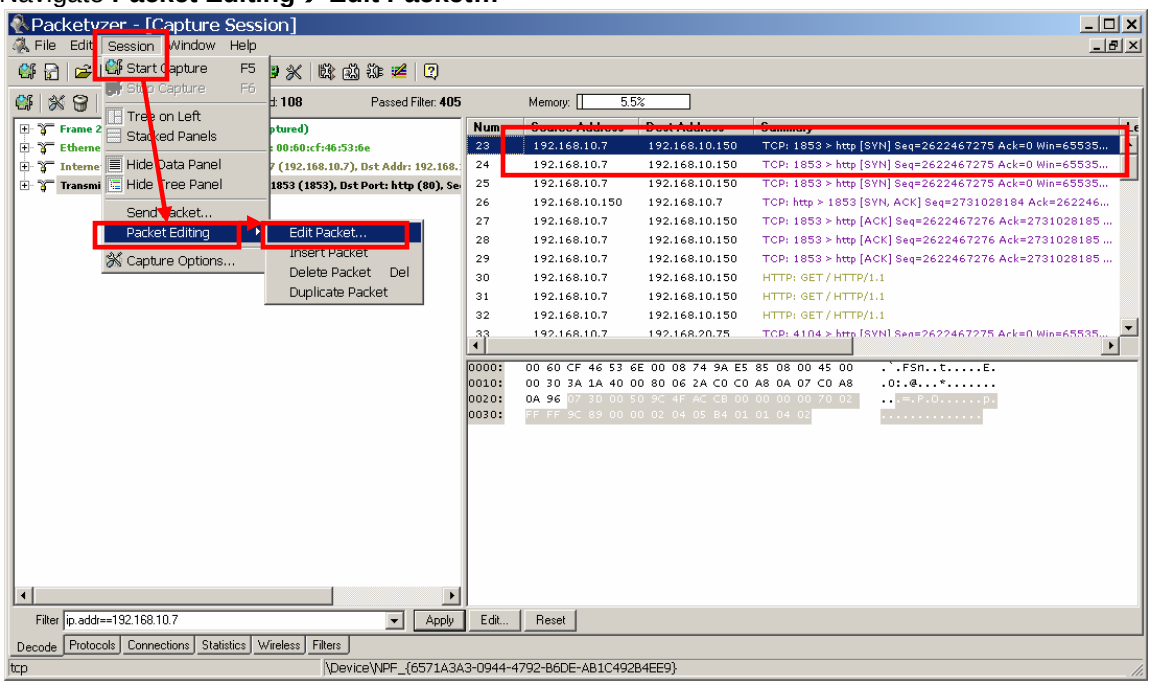
SYN Attack Detection

```
Alloc Fails - Seq buffers:       0    Alloc Fails - Ubufs:          0
Max sessions per bucket:         0    Max frames per session:       0
Max bytes buffered (sess):       0
```

Clear the log on Alteon:

```
>> Layer 7 Statistics# /info/clrlog
```

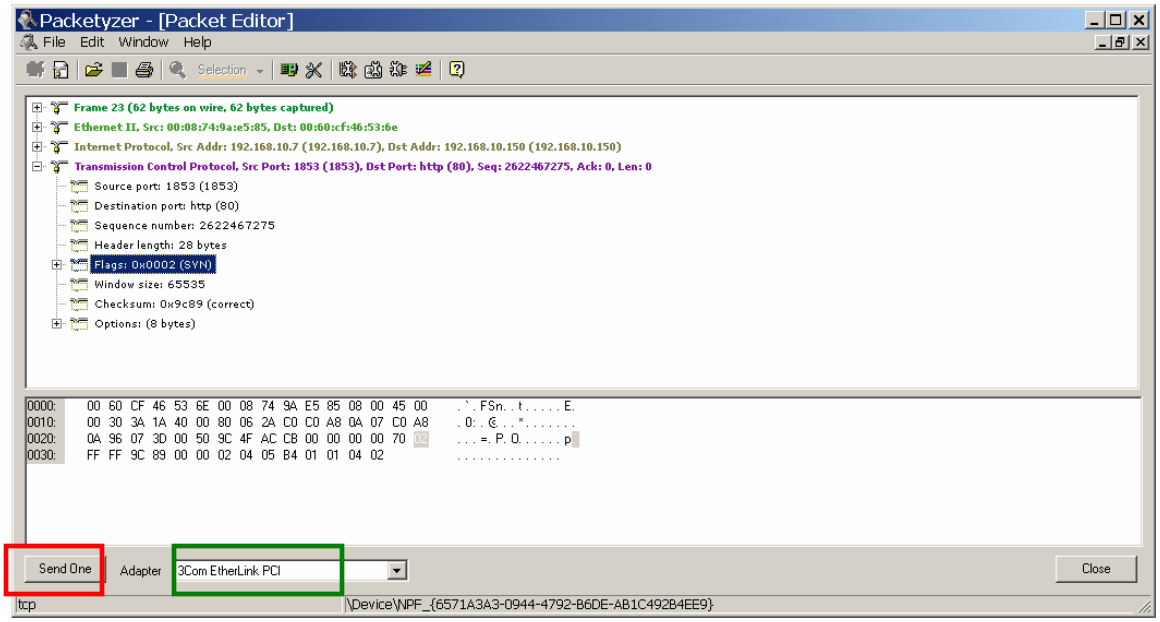
Locate a first SYN packet from PC (192.168.10.7) to web server (192.168.10.150) in the captured trace.
Highlight the packet.
Navigate **Packet Editing→ Edit Packet…**



 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

The **Packet Editor** window appears.
Make sure a packet From PC (192.168.10.7) to 192.168.10.150 with a SYN set was selected.
Select the appropriate **Adapter** and send several SYN packets by rapidly clicking **Send One** button:



Check the statistics for SLB. Note the number of half-opened connections:

```
>> Layer 7 Statistics# /stat/slb/layer7/maint
----------------------------------------------------------------------
Layer 7 maintenance stats:
Clients reset by switch on client side:            0
Clients reset by switch on server side:            0
Connection Splicing to support HTTP/1.1:           0
Aged delayed binding sessions:                     0
Half open connections:                            85
Switch retries:                                    0
Random early drops:                                0
Requests exceeded 9000 bytes:                      0
Invalid 3-way handshakes:                          0
Current SP memory units:     1344
Current SEQ buffer entries:     0    Highest:                    0
Current Data buffer use:        0    Highest:                    0
Current SP buffer entries:      0    Highest:                    0
Alloc Fails - Seq buffers:      0    Alloc Fails - Ubufs:        0
Max sessions per bucket:        0    Max frames per session:     0
Max bytes buffered (sess):      0
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Check the log on Alteon:

```
>> Layer 7 Statistics# /info/log
May  4 13:21:08 INFO    telnet/ssh-1: new configuration applied
May  4 13:21:09 NOTICE  slb: real service 192.168.20.75:80 operational
May  4 13:21:09 NOTICE  slb: real server 192.168.20.75 operational
May  4 13:21:09 NOTICE  slb: Services are available for Virtual Server
1:192.168.10.150
May  4 13:21:44 ALERT   slb: SYN attack detected: 6 new half-open
sessions per second
May  4 13:21:46 ALERT   slb: SYN attack detected: 5 new half-open
sessions per second
May  4 13:21:48 ALERT   slb: SYN attack detected: 6 new half-open
sessions per second
May  4 13:21:50 ALERT   slb: SYN attack detected: 6 new half-open
sessions per second
```

Check the SLB SYN attack information:

```
>> Information# /info/slb/synatk
SYN attack detection is currently running

SYN attack detection interval: 2 seconds
SYN attack detection threshold: 3 new half-open sessions/second
SYN attack warning fired: 16 times
```

Sending alerts to a remote syslog server

If we configure syslog to send messages to a remote syslog server, Alteon will send alerts to the syslog server.

Configuring syslog on Alteon

Enter the syslog configuration menu:

```
>> Configuration# /cfg/sys/syslog/
------------------------------------------------------------
[Syslog Menu]
      host    - Set IP address of first syslog host
      host2   - Set IP address of second syslog host
      sever   - Set the severity of first syslog host
      sever2  - Set the severity of second syslog host
      facil   - Set facility of first syslog host
      facil2  - Set facility of second syslog host
      console - Enable/disable console output of syslog messages
      cur     - Display current syslog settings
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Specify a remote syslog server (Linux server at 192.168.20.75 will be used as a syslog server in this example) using host command:

```
>> Syslog# host 192.168.20.75
Current syslog host:     0.0.0.0
New pending syslog host: 192.168.20.75
```

Apply and save the changes:

```
>> Syslog# apply/save
Request will first copy the FLASH "active" config to "backup",
 then overlay FLASH "active" with new config.
Confirm saving to FLASH [y/n]: y
New config successfully saved to FLASH.
```

Enabling syslog on the Linux machine acting as a Syslog Server

Enable syslog on Server to listen to remote clients.
Edit the **/etc/sysconfig/syslog** file to enable remote client logging. Add "**-r**" option to the SYSLOG_OPTIONS and save the file:

```
[root@linux7 user]# more /etc/sysconfig/syslog
# Options to syslogd
# -m 0 disables 'MARK' messages.
# -r enables logging from remote machines
# -x disables DNS lookups on messages recieved with -r
# See syslogd(8) for more details
SYSLOGD OPTIONS="-m 0 -r"
# Options to klogd
# -2 prints all kernel oops messages twice; once for klogd to decode,
and
#    once for processing with 'ksymoops'
# -x disables all klogd processing of oops messages entirely
# See klogd(8) for more details
KLOGD_OPTIONS="-x"
```

Restart the syslog:

```
[root@linux7 user]# /etc/init.d/syslog restart
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
```

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Verify Server is listening for remote clients:

```
[root@linux7 user]# netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
udp        0      0 *:1024                  *:*
udp        0      0 *:syslog                *:*
udp        0      0 *:sunrpc                *:*
```

By default all messages are written to `/var/log/messages` file.
To see messages added in a real time use **`tail –f /var/log/messages`** command. It will show the end of the `/var/log/messages` file and will continue to update on screen as messages are received:

```
[root@linux7 user]# tail -f /var/log/messages
May  4 01:48:16 linux7 syslog: syslogd shutdown succeeded
May  4 01:49:25 linux7 kernel: Kernel logging (proc) stopped.
May  4 01:49:25 linux7 kernel: Kernel log daemon terminating.
May  4 01:49:26 linux7 syslog: klogd shutdown succeeded
May  4 01:49:26 linux7 exiting on signal 15
May  4 01:49:26 linux7 syslogd 1.4.1: restart (remote reception).
May  4 01:49:26 linux7 syslog: syslogd startup succeeded
May  4 01:49:26 linux7 syslog: klogd startup succeeded
May  4 01:49:26 linux7 kernel: klogd 1.4.1, log source = /proc/kmsg
started.
```

Send a few SYN packets through the Packetyzer (enough to generate an alert).
Check the log (`/var/log/messages`) on the Server:

```
May  4 15:56:57 192.168.20.200 ALERT   WebOS <slb>: SYN attack detected:
6 new half-open sessions per second
```

Alteon has sent the alert to the remote syslog server.

 ©2005 Nortel Networks. All Rights Reserved

SYN Attack Detection

Appendix. Alteon configuration file

```
script start "Alteon AD3" 4  /**** DO NOT EDIT THIS LINE!
/* Configuration dump taken 13:41:29 Tue May  4, 2004
/* Version 10.0.30.7,  Base MAC address 00:60:cf:46:53:60
/c/sys
        idle 60
        tnet ena
/c/stp 1/off
/c/sys/syslog
        host 192.168.20.75
/c/ip/if 1
        ena
        addr 192.168.10.100
/c/ip/if 2
        ena
        addr 192.168.20.200
/c/slb/adv/synatk
        thrshld 3
/c/slb
        on
/c/slb/adv
        direct ena
/c/slb/real 1
        ena
        rip 192.168.20.75
/c/slb/group 1
        add 1
/c/slb/port 1
        client ena
/c/slb/port 7
        server ena
/c/slb/virt 1
        ena
        vip 192.168.10.150
/c/slb/virt 1/service http
        group 1
        dbind ena
/
script end  /**** DO NOT EDIT THIS LINE!
```

 ©2005 Nortel Networks. All Rights Reserved

Tech Tip
Alteon

SYN Attack Detection

Copyright © 2005 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globemark, and Alteon are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Limited.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: http://www.nortel.com/support

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu).

We welcome you comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: CRALT@nortel.com

Author: Kristina Senkova