

I don't have a firewall, proxy server, or Radius server. Can I still use this product?

You can still use Firewall Analyzer to simulate firewall logs and see how reports will look like when real-time data is used. Click the **Simulate** link in the [Settings tab](#) to begin sending sample log files to Firewall Analyzer.

How many users can access the application simultaneously?

This depends only on the [capacity of the server](#) on which Firewall Analyzer is installed. The Firewall Analyzer license does not limit the number of users accessing the application at any time.

How secure is the data that is sent to the web browser over the Internet?

Data sent from Firewall Analyzer is normally not encrypted and hence is readable if intercepted.

Firewall Analyzer runs in a web browser. Does that mean I can access it from anywhere?

Yes. As long as the web browser can [access the server](#) on which Firewall Analyzer is running, you can work with Firewall Analyzer from any location.

How do I buy Firewall Analyzer?

You can buy Firewall Analyzer directly from the [AdventNet Online Store](#), or from a [reseller near your location](#).

Is there a limit on the number of users or web sites that I can monitor?

There is no license restriction on the number of users or web sites that you can monitor. However, you may face performance issues when using [lower end machines](#) to run Firewall Analyzer.

What are the recommended system requirements for Firewall Analyzer?

It is recommended that you install Firewall Analyzer on a machine with the following configuration:

- * Processor - Pentium 4 - 1GHz
- * Disk Space - 1 GB
- * RAM - 512MB
- * Operating System - Windows 2000/XP, Linux 8.0/9.0
- * Web Browser - Internet Explorer 6.0, or Mozilla Firefox 1.0

Look up [System Requirements](#) to see the minimum configuration required to install and run Firewall Analyzer.

Does the installation of Firewall Analyzer make any changes to the firewall server configuration?

The installation of Firewall Analyzer does not make any changes to the firewall server configuration.

Can I install Firewall Analyzer as a root user?

Firewall Analyzer can be started as a root user, but all file permissions will be changed, and later you cannot start the server as another user.

When I try to access the web client, another web server comes up. How is this possible?

The [web server port](#) you have selected during installation is possibly being used by another application. Configure that application to use another port, or [change the Firewall Analyzer web server port](#).

Is a database backup necessary, or does Firewall Analyzer take care of this?

The [archiving feature](#) in Firewall Analyzer automatically stores all logs received in zipped flat files. You can configure archiving settings to suit the needs of your enterprise. Apart from that, if you need to backup the database, which contains processed data from firewall logs, you can run the database backup utility, **BackupDB.bat/.sh** present in the `<FirewallAnalyzer_Home>/troubleshooting` directory.

How do I see session information of all users registered to log in to Firewall Analyzer?

The session information for each user can be accessed from the [User Management page](#). Click the **View** link under Login Details against each user to view the active session information and session history for that user.

How do I configure my firewall to produce log files in WELF?

Firewalls usually need to be configured specifically to generate log files in WELF. The [Configuring Firewalls](#) section includes configuration instructions for some of the firewalls supported by Firewall Analyzer.

My firewall cannot export logs. How do I configure Firewall Analyzer to report on my firewall?

You can set up Firewall Analyzer to [import the logs](#) from the firewall at periodic intervals.

Does Firewall Analyzer store raw logs?

Raw [logs are archived](#) periodically, and stored as zipped flat files. You can load these archived log files into Firewall Analyzer at any time and generate reports based on them.

Why am I seeing empty graphs?

Graphs are empty if no data is available. If you have [started the server](#) for the first time, wait for at least one minute for graphs to be populated.

What are the types of report formats that I can generate?

Reports can be generated in HTML, CSV, and PDF formats. All reports are generally viewed as HTML in the web browser, and then exported to CSV or PDF format. However, reports that are scheduled to run automatically, or be emailed automatically, are generated only as PDF files.

Are IP addresses automatically resolved?

IP addresses are automatically resolved by connecting to the network DNS server.

Why are some traffic values shown as 0.0MB or 0.00%?

Since Firewall Analyzer processes log files as and when they are received, traffic values of 0.0MB or 0.0% may be displayed initially when the amount of traffic is less than 10KB. In such a case, wait until more data is received to populate the report tables.

What are the different formats in which reports can be exported?

Reports can be exported as PDF or CSV files. However, [reports are emailed](#) only as PDF files.

Why do the intranet reports show zero results?

Verify if intranet's have been configured correctly. If you have specified IP addresses that are not actually behind the firewall, you will get zero values in the reports.

Why don't trend reports take time values or top-n values into account?

Trend reports show historical data for the corresponding traffic statistics shown in the report. Hence time changes from the [Global Calendar](#), or top-n value changes from the **Show** bar on the report, do not affect these reports.

Why the Un-used Rules Report is empty?

To view the "Un Used Rules Reports", you need to configure Firewall Analyzer to fetch rules from device via Telnet or SSH. After this configuration the reports will be available. However, this advanced feature is available only for Premium License Users of Firewall Analyzer.

CheckPoint Firewall Reports

All the traffic reports are showing bytes value as zero?

Make sure you have set the Track value of your rules to **Account** in your CheckPoint management station. You can use Check Point Smart console to do the same. You can set the track value as *Account* for the rules that are allowing the traffic through your firewall's.

I am not getting VPN reports for CheckPoint firewall?

Firewall Analyzer looks for either the **vpn_user** or **peer gateway** attributes in the logs received from your CheckPoint firewall's to generate VPN reports.

Example log is as follows:

```
id=leafirewall time="23Oct2006 9:49:30" action="encrypt" orig="testing" i/f_dir="inbound" i/f_name="eth-s4p1 c0" has_accounting="1" product="VPN-1 & FireWall-1" __policy_id_tag="product=VPN-1 & FireWall-1[db_tag={C59340B0 - 6276-11DB-B086-00000000C2C2};mgmt=testing;date=1161594819;policy_name=RKR_Policy]" src="xxx.xxx.xxx.xxx" s_port="40555" dst="xxx.xxx.xxx.xxx" service="https" proto="tcp" rule="15" scheme="IKE" dstkeyid="0x31b52e56" methods="ES P: AES-256 + SHA1" peer gateway="mygateway" community="SECU" start_time="23Oct2006 9:49:30" segment_time="23Oct 2006 9:49:30" elapsed="0:00:09" packets="3" bytes="180" client_inbound_packets="3" client_outbound_packets="0" server_inbound_packets="0" server_outbound_packets="3" client_inbound_bytes="180" client_outbound_bytes="0" server_inbound_bytes="0" server_outbound_bytes="360" client_inbound_interface="eth-s4p1c0" server_outbound_interface="eth-s3p1c0" __pos="7" __nsons="0" __p_dport="Unknown"
```

All the received logs are stored in `Firewall_Analyzer_Home\server\default\archive\` directory. You can browse through those logs to troubleshoot the problem.

If you find vpn related logs with other fields, then kindly send us the sample logs by uploading them to the following link: <http://bonitas.adventnet.com/upload/index.jsp?to=support@fwanalyzer.com>

I am not getting Attack Reports in CheckPoint firewall?

Firewall Analyzer looks for the attribute **attack** in the CheckPoint firewall logs to generate the attack reports.

Firewall Analyzer shows the destination site (example: www.yahoo.com) but it is not showing the complete URL (example: www.yahoo.com/index.html)?

It looks for the attribute **resource** in the log.

Example log is as follows:

```
id=leafirewall time="16Aug2006 7:43:56" action="accept" orig="AHFW_1" i/f_dir="outbound" i/f_name="eth0" has_accounting="1" product="VPN-1 & FireWall-1" __policy_id_tag="product=VPN-1 & FireWall-1[db_tag={55E82635-247B-44 B7-9E29-42EDE0F57E2C};mgmt=FW_MGMT;date=1155671079;policy_name=N2H2_Filtered]" rule="22" rule_uid="{5A131CD7-BCBA -4859-AB39-43594A24931A}" rule_name="HTTP Outbound" service_id="http" src="xxx.xxx.xxx.xxx" s_port="2624" dst="xxx.xxx.xxx.xxx" service="http" proto="tcp" xlatesrc="xxx.xxx.xxx.xxx" xlatesport="57700" xlatedport="Unknown" NAT_rulenum="94" NAT_addtnl_rulenum="internal" resource="http://www.yahoo.com/index.html" start_time="16Aug2006 7:43:56" segment_time="16Aug2006 7:43:56" elapsed="0:00:00" packets="11" bytes="1161" client_inbound_packets="6" client_outbound_packets="5" server_inbound_packets="5" server_outbound_packets="6" client_inbound_bytes="753" client_outbound_bytes="408" server_inbound_bytes="408" server_outbound_bytes="753" client_inbound_interface="eth0" client_outbound_interface="eth0" server_inbound_interface="eth1" server_outbound_interface="eth1" __pos="7" __nsons="0"
```

Why do I see zero results for kilobytes transferred in the reports for Check Point firewall?

This could be happening because bandwidth information is not being captured in the log file. Ensure that your Check Point firewall has been configured to generate both regular and accounting log files. While regular log files contain information regarding firewall activity, the accounting log file contains the bandwidth and session information. Please refer the [Configuring Check Point Firewall's](#) section for help on creating the accounting log file.

I am getting only Unknown Events in Event Overview graphs in the dashboard?

CheckPoint firewall logs do not have the priority or severity fields. Event Overview graph groups Events based on severity. As there is no severity in check point logs, Firewall Analyzer puts default value as Unknown severity and hence Event Overview shows only Unknown Events. If you drill down that group or by clicking the More link, you can get complete Events.

Cisco PIX Firewall Reports

I am not seeing Traffic reports in Cisco firewall's?

1. In your Cisco PIX command line interface execute the command **show logging** and check the trap logging value.
2. The trap logging should be set to informational for traffic logs to be generated from Cisco PIX firewall's Execute the command **logging trap informational** to set the trap logging to informational.
3. Ensure that no logs are disabled in Cisco PIX by executing the command **show logging disabled**
4. Commonly, logs with id 302013,302014,302015 and 302016 are dealing with traffic. Make sure those ids are not disabled in your cisco firewall. If they are disabled then execute the command **logging message** to enable them.

I am not getting VPN reports for Cisco firewall's?

We can setup two kind of VPN's in Cisco firewall's as below.

1. **Remote Host VPN:**

This is between a User PC and the Cisco firewall's. User PC could be anywhere in the Internet. There are various technologies used to accomplish the same. Firewall Analyzer supports the following types.

- o **IpSec:**

Firewall Analyzer supports IpSec remote host vpn in Cisco firewall's. Following are the sample logs generated:

Cisco PIX:

```
20_12_2005_09_00_20:<166>Dec 20 2005 09:52:14: %PIX-6-109005: Authentication succeeded for user 'john' from xxx.xxx.xxx.xxx/0 to xxx.xxx.xxx.xxx/0 on interface outside
```

```
20_12_2005_09_00_20:<166>Dec 20 2005 09:52:16: %PIX-6-602301: sa created, (sa) sa_dest=xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x1e01c9b1(503433649), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 46
```

```
20_12_2005_09_00_20:<166>Dec 20 2005 09:52:16: %PIX-6-602301: sa created, (sa) sa_dest=xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x94e99fdc(2498338780),V sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 45
```

20_12_2005_09_00_20:<166>Dec 20 2005 09:55:24: %PIX-6-602302: deleting SA, (sa) sa_dest=xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x1e01c9b1(503433649), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 46

20_12_2005_09_00_20:<166>Dec 20 2005 09:55:24: %PIX-6-602302: deleting SA, (sa) sa_dest=xxx.xxx.xxx.xxx, sa_prot= 50, sa_spi= 0x94e99fdc(2498338780), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 45

Cisco ASA:

<166>:Apr 10 15:26:51 CDT: %PIX-vpn-6-602303: IPSEC: An inbound remote access SA (SPI= 0x2C4009CD) between xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx (user= ARNOLD) has been created

<166>:Apr 10 22:13:21 CDT: %PIX-vpn-6-602304: IPSEC: An inbound remote access SA (SPI= 0xA57F6150) between xxx.xxx.xxx.xxx and xxx.xxx.xxx.xxx (user= ARNOLD) has been deleted

<164>:Apr 10 20:13:23 CDT: %PIX-auth-4-113019: Group = TUMBUVPN, Username = ARNOLD, IP = xxx.xxx.xxx.xxx, Session disconnected. Session Type: IPSecOverUDP?, Duration: 4h:46m:39s, Bytes xmt: 1270639, Bytes rcv: 4292608, Reason: User Requested

- **PPTP:**

Firewall Analyzer supports PPTP VPN between Cisco firewall and user's PC. Following are the sample logs generated:

<133>Oct 20 2005 20:57:10: %PIX-6-603108: Built PPTP Tunnel at inside,tunnel-id = 25, remote-peer =xxx.xxx.xxx.xxx, virtual-interface = 1,client-dynamic-ip = xxx.xxx.xxx.xxx, username = king,MPPE-key-strength = number

<134>Oct 20 2005 20:58:01: %PIX-6-603109: Teardown PPPOE Tunnel at interface_name, tunnel-id = 25,remote-peer = xxx.xxx.xxx.xxx

<134>Oct 20 2005 20:53:21: %PIX-6-603104: PPTP Tunnel created, tunnel_id is 26, remote_peer_ip is xxx.xxx.xxx.xxx, ppp_virtual_interface_id is 2,client_dynamic_ip is xxx.xxx.xxx.xxx, username is king, MPPE_key_strength is None

<134>Oct 20 2005 20:58:01: %PIX-6-603105: PPTP Tunnel deleted, tunnel_id = 26, remote_peer_ip = xxx.xxx.xxx.xxx

2. **Site-To-Site VPN:**

This vpn connection will be established between firewall to firewall. In most of the cases, this connection would have been established before the Firewall Analyzer installation. Also Cisco firewall's do no hint about the traffic that is going through this Site To Site VPN tunnel in the logs. So Firewall Analyzer is **not supporting** this type of VPN connection now.

My Attack Reports displays "No Data Available"?

Cisco firewall's have inbuilt Intrusion Detection Systems (IDS) that detects the attacks. Firewall Analyzer supports all

attack logs in Cisco firewall devices. All the attacks are identified by the cisco ids from 400000 to 400050. Apart from these logs, Firewall Analyzer also identifies supports ID's like 106016, 106017 etc. So if you find Attack reports empty there is a very valid chance that you have not received any attacks. To verify that you can go to `Firewall_Analyzer_Home\server\default\archive\` and search for the above ID's.

My Virus Reports are never getting populated?

In Cisco firewall's, all the doubtful activities will be identified as attacks and hence you will see all of them in Attack Reports. No Virus logs are given by Cisco Firewall's and hence there are no Virus Reports. You can very well remove the listing of Virus reports through report customization.

My Admin Reports displays "No Data Available"?

Firewall Analyzer reports login/logout attempts by searching the Cisco firewall logs for message ids like 611101,611102, 611103, 605004, and 605005. Take a look at the logs available at `Firewall_Analyzer_Home\server\default\archive\` directory in case of any discrepancy.

NetScreen Firewall Reports (Syslog)

I am not getting any traffic reports. All SENT and RECEIVED values are shown as zero?

1. Make sure you have enabled traffic logs in your Netscreen.
2. In certain versions of NetScreen firewall there is an option to log the completed transaction whereas the other option is to log the initiated transaction. We recommend you to select the completed transaction option and deselect the initiated transaction option. This is because you can get the SENT and RECEIVED values only when the transaction is completed. You will find this check box while editing the rule.
3. Make sure you have enabled all logging levels upto informational. Because informational level logging includes traffic information

The VPN reports for my NetScreen firewall's are not getting populated?

Firewall Analyzer searches for **action=Tunnel** attributes in the NetScreen firewall logs to generate VPN reports.

I am not getting Virus reports for NetScreen firewall's?

Firewall Analyzer searches for the attribute **Virus** in the NetScreen firewall logs to generate Virus reports. Take a look at the log files available under `Firewall_Analyzer_Home/server/default/archive/` directory in case of any discrepancy.

Other Firewall Reports (Sonicwall, Fortigate, and all other firewall's that support WELF)

My reports show *No Data Available*

This means Firewall Analyzer has discovered your firewall and is able to recognize the logs. By default, as soon as you login, Firewall Analyzer shows data from current day's 00:00:00 hrs to current time of the machine where you are running Firewall Analyzer. There is a possibility that the firewall logs timestamp could be different from the Firewall Analyzer's timestamp. So just check `Firewall_Analyzer_Home/server/default/archive/` directory to view the firewall logs timestamp.

I am not getting any traffic reports?

Make sure you have enabled traffic logs and have set your logging level to informational. This is because most of the firewall's generate traffic logs only when logging level is set to informational.

The VPN reports for my firewall does not show any data?

Firewall Analyzer searches for attributes like **vpn=** or **vpnpolicy=** to generate VPN reports. So please verify whether your firewall logs have these attributes.

The Virus Reports for my firewall is not getting populated?

Firewall Analyzer searches for the attributes like **virus=** to generate the virus reports. Example logs are given below.

```
id=firewall time="2005-06-13 20:48:37" fw=FGT4002803033009 pri=5 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx
src_int=n/a dst_int=n/a service=http status=passthrough from="n/a" to="n/a" file=trace.exe virus="Suspicious"
msg="The file trace.exe is infected with Suspicious.
ref http://www.fortinet.com/VirusEncyclopedia/search/
encyclopediaSearch.do?method=quickSearchDirectly&virusName=Suspicious.";
```

The Attack Reports for my firewall is not getting populated?

Firewall Analyzer searches for the attributes like **attack=** or **attack_id=** to generate attack reports. Example logs are given below.

```
17_08_2005_16_54_03:id=firewall time="2005-08-18 00:59:03" fw=FGT4002803033026 pri=1 attack_id=101974095
src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx
src_port=110 dst_port=58714 src_int=n/a dst_int=n/a status=detected proto=6
service=58714/tcp msg="misc: MS.Outlook.GMT.BufferOverflow,repeated 2 times[Reference:
http://www.fortinet.com/ids/ID101974095]";
```

I am not getting complete URLs for the destination sites?

Firewall Analyzer combines values of the fields like **dst/dstname** and **arg** to form the complete url. Kindly check whether your firewall generates the same in the log files available under *Firewall_Analyzer_Home/server/default/archive/* directory. Example logs are given below.

```
1902-01-16 08:52:47 Local0.Info 192.168.14.3 "id=firewall sn=0006B10C5210
time="2006-01-06 15:53:30 UTC" fw=myfirwall pri=6 src=xxx.xxx.xxx.xxx dst=xxx.xxx.xxx.xxx proto=tcp/http
op=GET sent=1533 rcvd=512 result=200 dstname=c.microsoft.com arg=/trans_pixel.asp?
source=msdn&TYPE=PV&p=library_en-us_cpguide_html&URI=%2flibrary%2ft
```