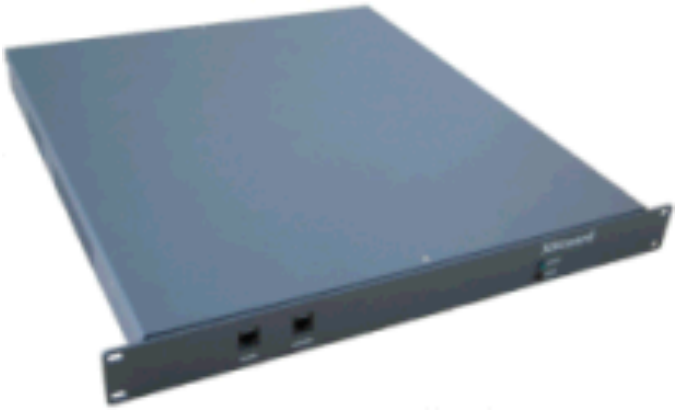
Black Box Defender Standard and Pro

Intrusion Prevention System



KEY BENEFITS

Real-time Intrusion Prevention
Instead of waiting for an attack to take place, the Defender blocks an attack before it can intrude the network.

Maintenance Free
All the maintenance and updates of the engine and rules are done central which saves the customer time, effort and money.

Protects against unknown attacks
The Defender to detect known as well as unknown vulnerabilities, so called zero-day exploits.

Unhackable
The Defender uses bridging technology making it unapproachable and invisible while functioning.

Most affordable IPS solution

Introduction

The wide availability of broadband connections has lead to a boom in companies being constantly on-line. This increased connectivity also imposes increased security risks. Most companies still rely solely on their firewall to stop attacks. But internet security is more then just a firewall. Most attacks are able to slip through the firewall and reach the network behind.

Today's major threats for network environments are hackers and worms.

Both threats are capable of crippling an entire computer system causing applications to malfunction or stop completely. The direct costs associated with events caused by these threats can be massive. The indirect costs may be even higher since confidential and personal information can become general available causing damaged customer faith. To re-establish the good name and reputation of the company usually requires a massive marketing effort.

Defender stops the threats before they reach your network.

Current security systems that protect networks against intruders are based on detection. These so-called Intruder Detection Systems (IDS) raise an alarm when they detect an intruder but most of the time they are too late for prevention. Although IDS can sometimes be interfaced with a firewall to perform basic automatic protection functionality they require continuous effort. This along with the expertise needed makes IDS expensive to manage and support.

Intrusion Prevention (IPS) can both detect an attack and block the attack itself. An IPS only blocks a session containing an attack or illegal traffic. This means legal traffic from the same sender will be allowed to enter the network and not all traffic from that person will be blocked. The advantage of this feature is that networks have a better availability for external parties.

The basic difference is that an IDS reacts to a situation, while an IPS system prevents it from happening.

Worms

A worm is a program that uses malicious code to automatically detect and abuse flaws in a system. The most well known worms are the blaster and slammer worm.

Open door

There is little or no awareness for intrusion protection. Most companies have a false sense of security. They are unaware of the openings a firewall and anti-virus software leave in their network.

A firewall protects a network from non-friendly users, by construction of a virtual 'wall'. It intentionally leaves some 'doors' in the 'wall' open to enable e-mail, web traffic or other data to pass through. Unfortunately most hackers and worms also enter networks through these doors.

Intruder Prevention Systems (IPS) are designed to stop these attacks. IPS protects servers and applications that are intentionally accessible through the firewall. All traffic is analysed before passing and based on this analysis it decides what to block and what not.

The Defender Solution

Defender effectively protects against hackers and worms, protecting servers and applications that are intentionally accessible through the firewall. All traffic is analysed before passing and the Defender clearly decides what to block and what not. Placed in front of a network the Defender does not rely or interfere with systems on that network.
Defender uses stateful pattern matching with protocol decode-based analysis, and has a global service for automatic updates. This means that Defender uses signatures to detect and block network attacks, and also verifies the integrity of the used protocols to detect possible unknown attacks. Updates are done automatically (worldwide) and all new vulnerabilities are blocked when they become public. Our team of security experts constantly watches all the developments of potential vulnerabilities and security threats. While it takes most IDS experts hours to define correct defences in an IDS or firewall; the Defender system is managed remotely and is automatically updated.

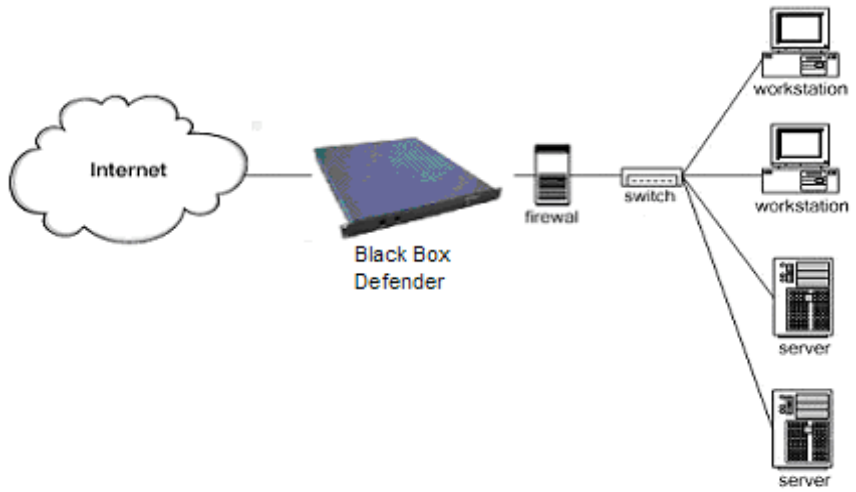
There is no need for expensive security experts. The Defender comes pre-installed and needs no maintenance.

With Defender your Internet infrastructure is protected against exploits and vulnerabilities in your own systems and software (components). The profiles of these vulnerabilities are stored in Defenders internal database. In fact this database is Defenders beating heart. Since new vulnerabilities are detected every day, the database is updated everyday. This updating is handled by the Defender Management Console. The principle is very similar to your anti-virus software. However, your Defender receives new profiles by the initiative of the Management Console. Part of the updating process is a sanity and integrity check of your Defender. This means that the proper functioning of your Defender will be regularly checked.

Stateful pattern matching
Pattern matching is the technique o looking for fixed patterns in data streams to detect known exploits and anomalies.

Protocol analysis
Protocol analysis performs advanced calculations on each packet by looking a the packaging of traffic. This technique verifies the headers to ensure that the packet contains what it says it does.

Defender involves insertion of an additional device in the internet-access line in series with the firewall. This device analyses all TCP/IP command-strings coming from the internet and will block those which contain a cyber-attack patterns.



Defender is comparing commands with more than 4000 known malicious attack patterns. Defender is using leading-edge technological solutions to perform this analysis in real-time in the current broadband internet environment.

The Defender principle is simple: just catch all the messages that pass and check if they are a threat to the infrastructure that must be protected. Although this principle is simple, it takes some effort to get it done. Furthermore there are some side-issues to consider. For one, it should not be possible to communicate directly with the Defender. If this were possible, the Defender itself could be attacked. Therefore the Defender has no IP-address and is completely invisible. This makes it impossible to detect the presence of the Defender. And since there is no way to tell that an Defender is installed, it cannot be attacked!!

Layer 2 Bridge
The feature that makes it possible for the Defender to work without an IP-address is called *Bridging*. A bridge is a way to connect two network segments together without using specific protocols. Packets are forwarded based on Ethernet address, rather than IP address. This technique makes the Defender invisible and unreachable for other machines on the network.

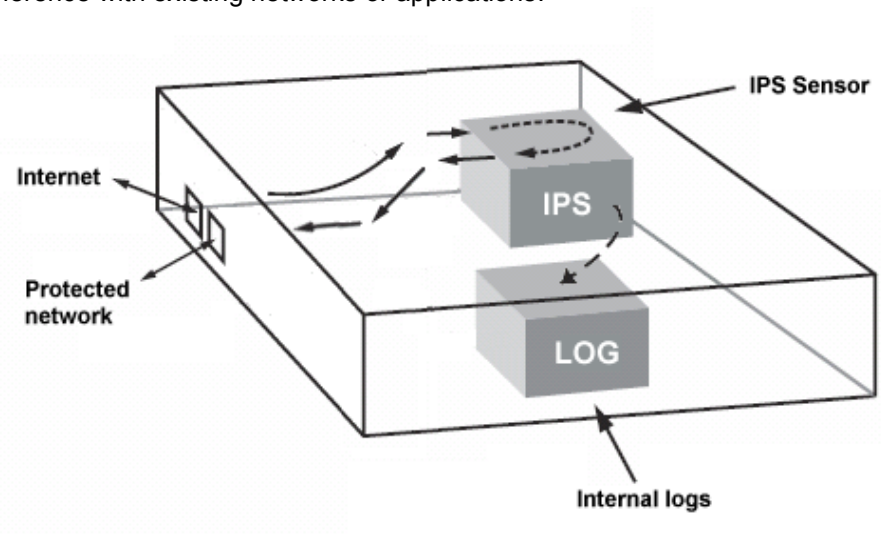
It is a genuine 'invisible' protective shield against malicious cyber-attacks.

Before Firewall
The advantage of placing the Defender in front of the firewall is that the firewall itself is protected from possible attacks. It also reduces the load generated on the network. The disadvantage is that the Defender generated alerts for attacks that could be harmless for your network or which were normally blocked by the firewall.

After Firewall
The advantage of placing the Defender behind the firewall and/or other security products is that it allows you to see which attacks aren't blocked by your existing environment.
The disadvantage is that your firewall and possible other products are not protected against possible attacks.

Sensor: Filtering mechanism

Defender has 2 Network Interface Cards (NIC). The first NIC is connected to Internet, the second one is connected to the network that is to be protected. Defender is completely transparent as long as no hostile messages are detected. Due to this transparency, there is no interference with existing networks or applications.



Defender re-assembles the IP packages from the incoming NIC until the complete message is available. Once the complete message is available, this message is checked to see if it causes a threat to the network that is to be protected. If the message is considered “safe”, it is forwarded through the second NIC. If the message is not “safe”, it is dropped. In this case, the originator will not receive a reply to the message resulting in a time-out at the originator’s end. The fact that the message is dropped also results in an entry in the hostile-message log file. Since this entry also contains the date, time and the IP address of the originator it can be used to retrieve the originators identity.

Time to patch

The number of vulnerabilities discovered in complex software and software applications in increasing rapidly and the possibilities for hackers to attack IT infrastructures are increasing in line with that development.

Software industry is frantically developing patches to make repairs to the revealed security flaws, however the time lapse between the discovery of a software error and the release of a viable and tested patch may still be several weeks, sometimes even months.

Meanwhile the security flaw has become widely known and hackers and worms can do their malicious work as intruders in your system.

Impact may vary from friendly visits and information or bandwidth theft to genuine system-control takeovers and software and data corruption in all kind of forms. Besides possible direct damage to the operation intrusions always have the same effect on the victim company; feelings of privacy violation and severe public damage to the company’s reputation.

Internal logs

The Defender queues alert information on an internal storage device. If there is enough bandwidth available on the Internet connection and when a connection is established with the Management Server, the Defender sends the log files to the server. In case of high bandwidth usage, for example during a DoS attack, or when the Defender is unable to reach the server the logs are kept on the internal drive until these issues are resolved.

Defender takes away these risks because the signatures of these security flaws are directly implemented in the system far before the necessary patches are released.

False Positives

Although there is no 100% guarantee that false positives never happen they are actively managed. Every message that is blocked by any Defender is reported back to the management system. There, the message is analyzed. If a message was blocked that is 'new' to the management system (and therefore was never blocked before), the message is anonymously forwarded to the 'attack-signature-team' for further analyses. If the experts from the attack-signature-team conclude that this was indeed a false-positive, the attack-signature is updated to prevent repetition. This scheme doesn't guarantee the prevention of false-positives, but by actively managing them, all Defender users gain from each others experience.

Denial of Service

There are two types of DoS attacks. One is based upon using all the targets processor capacity (e.g. by uploading malicious code to the target or executing malicious commands) so no requests can be handled. The other type aims to cripple the target by overloading it with messages. DoS attacks of the first kind are handled by Defender since it detects the malicious code or commands and it does not reach the target. A Dos attack of the second type is a different matter. In this case Defender will take the heat. In fact, a "well-engineered" DoS attack will most likely cripple Defender. When this happens, the NICS will short circuit and the Defender Management Console will detect that Defender is taken off-line. This will result in the proper alarm messages indicating that an exceptional situation is at hand.

The NIC Switchover

Defender is specifically designed not to interfere with the customers existing infrastructure. A special feature that makes this possible is the NIC Switchover (NICS), it takes care of a malfunctioning Defender.
Whenever the Defender is no longer available, e.g. due to a power failure, hard disk crash etc., the NICS establishes a direct physical connection between the incoming and outgoing UTP cables thereby "bypassing" Defender. Although the network is no longer protected by Defender, network communication is still possible!
It is obvious that such an event must be detected, the fact that the network is no longer protected may result in a catastrophe. This detection is handled by the Defender Management Console. Every two minutes, the Defender Management Console sends a little message to the Defender to check whether or not the Defender is still alive (in fact the message is send to the network behind Defender, however Defender detects that it is a management message and it handles the response itself). If there is no (valid) response received, the Defender management Console knows that "there is something wrong".

Upon this event, the Defender Management Console sends out alert e-mails and text messages to mobile phones, thereby ensuring that proper actions may be taken.
If a situation whereby the network is no longer protected by Defender is considered to be unacceptable, than Defender can be used without the NICS by simply connecting the Internet and de network directly to NIC-1 and NIC-2 respectively!!

Active IDS not IPS

Most IPS systems on the market today are in fact not real IPS but Active IDS. An active IDS is a standard IDS system combined with an external or integrated firewall. The IDS detects an attack as soon as it passes the sensors, and after detection it changes the settings of the firewall, router or switch policies to block the incoming attack.

This has a couple of major drawbacks:

- When a "false positive" occurs, the whole network could become unreachable, and the administrator will have to change settings by hand to resolve this problem.
- There is a realistic chance an attack can be done successfully before a new policy becomes active in the firewall, switch or router.

Because of the use of firewall blockages it becomes much easier to apply a DOS (Denial of Service) attack; the so called "spoofing".

Zero Maintenance

Defender takes a few minutes to install, does not require specialist intervention and does not interact with the existing network infrastructure. It is in fact a real ‘plug-and-play’ service that forms a true ‘invisible’ shield against cyber-intrusions.

When installing the Defender Service, a device is inserted between the internet access point and the network; this device is the Defender client system.
When it is installed it will within minutes automatically fetch all the possible attack patterns from the central server network. From that moment on the infrastructure is fully protected against attacks from cyber-criminals and worms coming in from the internet.

Defender is always connected to the Defender global management network and to the Defender security database. The continuous process of updating this database ensures full protection of your network at all times against known and unknown attacks.

Automatic updates

The power of the service solutions is that all Defenders are identical, and they will all be updated within minutes whenever a new software error or attack pattern has been made available in the central database. There is no need to wait for development of software patches or to schedule software patching at the customer to restore protection to the initial level, as it just takes the attack pattern to be loaded in to database.

Management Console

The management of your Defender is handled by the Defender Management Console. The most important task of the Defender Management Console is to update the vulnerability database in your Defender, ensuring that you are protected against the latest threats (comparable to updating a virus-profile database used by anti-virus software).
The Defender Management Console also handles the reports about (possible) attacks on your infrastructure that your Defender generates. The Defender Management Console collects the data and sends it to the reporting server where it is processed before it is send to you.
Furthermore the Defender Management Console monitors the status of your Defender. Every two minutes, the Defender Management Console questions your Defender to see whether or not it is 'alive' and if so if it is functioning as it should be. Whenever a status change is detected that might have any influence on the protection of your infrastructure, this is signalled so proper action can be taken.

User Portal

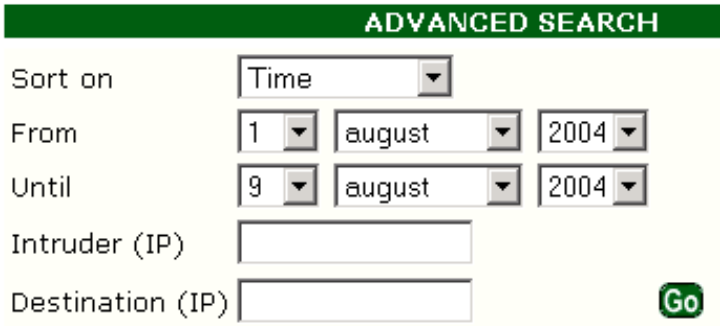
Defender automatically provides concise on-line management reports concentrating on actual events.

As a service feature and for protection enhancement, there is no local interface with the Defender client system. Customers have protected access to the User Portal on the central Defender system to obtain overviews and statistical report on the type and origin of attacks that Defender has effectively blocked.

Also the management server can send out alarm messages (e-mail, SMS) to the client in case of 'excessive' amounts of malicious traffic.

Logs

Through the User Portal, customers can browse and explore the events that have taken place on the Defender. The web interface is instinctive and easy to use. There are options to make reports based on a specific time line, intrusion type, intruder or destination (target).



The interface creates easy to use reports that can be explored and displayed in a number of different ways.

Intrusion type	Count	Details
sqlslammerudp	7800	Report
n10258	84	Report
xsa353001	4	Report
Webdav1	3	Report
xsa20249	3	Report
xsa8035	1	Report

row 1 to 6 of 6

Report of periode 1 august 2004 to 11 august 2004 sorted by time

Back to query

Date	Time	Until	Intruder	Destination	Port	Count	Type	Details
2004-08-11	00:17:03	06:28:53	194.151.226.36	172.24.164.35	25	13	n10258	Data
2004-08-10	22:27:26	22:27:41	216.204.78.58	172.24.164.44	80	8	xsa20249	Data
2004-08-10	11:10:58	23:40:47	194.151.226.36	172.24.164.35	25	26	n10258	Data
2004-08-06	20:50:54	20:50:58	194.206.215.23	172.24.164.43	80	3	xsa20249	Data
2004-08-06	00:06:11	20:52:32	194.151.226.36	172.24.164.35	25	39	n10258	Data
2004-08-05	16:38:53	16:39:16	80.131.221.194	172.24.164.45	80	3	xsa8035	Data
2004-08-05	00:31:10	23:43:43	194.151.226.36	172.24.164.35	25	48	n10258	Data
2004-08-04	00:35:58	23:54:43	194.151.226.36	172.24.164.35	25	46	n10258	Data
2004-08-03	13:12:34	23:59:41	194.151.226.36	172.24.164.35	25	23	n10258	Data
2004-08-03	12:53:20	15:05:42	80.127.109.34	172.24.164.43	80	2	xsa8035	Data

row 1 to 10 of 10

When going to the deepest level, even the packet that is blocked and that contains the attack attempt is revealed.

Blocked entries of intruder 194.151.226.36 using n10258
on 2004-08-11 from 00:17:03 until 06:28:53

Time	Intruder	Destination	Port	Blocked entry
06:28:53	194.151.226.36	172.24.164.35	25	MAIL FROM:<Jimjam|jimjam@web-net.com> SIZE=2452
05:28:22	194.151.226.36	172.24.164.35	25	MAIL FROM:<Jimjam|jimjam@web-net.com> SIZE=2452
04:44:41	194.151.226.36	172.24.164.35	25	MAIL FROM:<Jimjam|jimjam@web-net.com> SIZE=2452
04:05:03	194.151.226.36	172.24.164.35	25	MAIL FROM:<Jimjam|jimjam@web-net.com> SIZE=2452
03:43:14	194.151.226.36	172.24.164.35	25	MAIL FROM:<Jkent38|jkent38@webtv.net> SIZE=2340

row 1 to 5 of 13

Next

Specifications

Ports

Configuration	:	RS232 port, DB-9 connector
Interfaces	:	10/100/1000 Ethernet ports (RJ-45 connectors)

Storage

Hard disk	:	40 GB storage for logs

Power

100-240 VAC. 350W

LED indicators

Power supply and IPS Active

Chassis

1U rack-mountable (standard 19-inch rack)

Dimensions

Height	:	1 U
Width	:	19 “
Depth	:	19 “
Weight	:	8 kg

Features and Characteristics:

- Active, real time protection against malicious visitors.
- Multi Operating System protection
- Multi protocol protection: HTTP, FTP, SMTP, POP3, IMAP, DNS, SMB etc.
- Automatically updated with latest vulnerability threats.
- Monthly report about blocked messages that would have caused a threat to your infrastructure.
- Invisible for the outside world.
- Active status monitoring and reporting (e-mail, text messaging on mobile phone).
- Communication between Defender and the Management Console using 1024 bit encryption key.
- Network Interface switchover in case of power or other system failure – Defender disconnects itself and passes all messages without checking them, notification is send within three minutes (e-mail, text message).
- No configurable parameters: Plug and Protect Installation procedure of less than two minutes.

About the team behind Defender

Our Defender Strike Team based in The Hague, The Netherlands specialises in active security solutions.

Defender Strike Team has its roots in consultancy and started as offspring off an ICT consultancy company founded in 1996. Network security was adopted as a special service because of the increasing demand for these services from customers. The Defender Strike Team consists of specialist from within the security world. They all have experience and knowledge of the current threats and risks of the internet.

Defenders IPS systems are protecting companies in various sectors such as government, insurance and banking.

Order information

To order please look on the website (www.blackbox.com) to locate a sales representative or contact Black Box directly at:

Black
Box Network Services

Tel.: +31-(0)30-241 77 77
Fax.: +31-(0)30-241 47 46
Mail: info@blackbox.nl

Mission Statement

The current security market is targeted a detecting and resolving vulnerabilities or business computer networks. We at Black Box believe that it is more important to stop intruders at the front door, instead o resolving problems that have already occurred. We provide innovative solutions for customers, and use our security knowledge to prevent problems instead of detecting them.

Innovation is the keyword within our company.