Yugoslav Journal of Operations Research
18 (2008), Number 1, 109-122
DOI: 10.2298/YUJOR0801109D

AN INTRUSION PREVENTION SYSTEM AS A PROACTIVE SECURITY MECHANISM IN NETWORK INFRASTRUCTURE

Nenad DULANOVIĆ

General Staff of Serbian Armed Forces
Belgrade, Serbia
nenad.dulanovic@vj.yu

Dane HINIĆ

General Staff of Serbian Armed Forces
Belgrade, Serbia
dane.hinic@vj.yu

Dejan SIMIĆ

Faculty of Organizational Sciences
University of Belgrade, Belgrade, Serbia
dsimic@fon.bg.ac.yu

Received: July 2005 / Accepted: April 2008

Abstract: A properly configured firewall is a good starting point in securing a computer network. However, complex network environments that involve higher number of participants and endpoints require better security infrastructure. Intrusion Detection Systems (IDS), proposed as a solution to perimeter defense, have many open problems and it is clear that better solutions must be found. Due to many unsolved problems associated with IDS, Intrusion Prevention Systems (IPS) are introduced. The main idea in IPS is to be proactive. This paper gives an insight of Cobrador Bouncer IPS implementation. System architecture is given and three different Bouncer IPS deployment modes are presented. The Bouncer IPS as a proactive honeypot is also discussed.

Keywords: Intrusion prevention system, bouncer, firewall.

1. INTRODUCTION

The expansion of the Internet and e-Commerce has made organizations more vulnerable to electronic threats than ever before. With the increasing quantity and sophistication of attacks on IT assets, companies have been suffering from breach of data, loss of customer confidence and job productivity degradation, all of which eventually lead to the loss of revenue. According to the 2004 CSI/FBI Computer Crime and Security survey [1], organizations that acknowledged financial loss due to the attacks (269 of them) reported $141 million lost, and this number has only grown since. Moreover, as unskilled, unmanned attacks such as worms and viruses multiply, the probability of attack approaches 1 for every organization. The question therefore shifts from whether an attack will occur, to when an attack will occur. Thus, a sound IT security plan is more important than ever, and the protection provided by current and emerging Intrusion Prevention Systems (IPS) is becoming a critical component [2, 3, 4, 5].

IPS utilizes IDS algorithms to monitor and drop or allow traffic based on expert analysis. These devices normally work at different areas in the network and proactively police any suspicious activity that could otherwise bypass the firewall. IPS “firewalls” can intelligently prevent malicious traffic from entering/exiting the firewall and then alert administrators in real time about any suspicious activity that may be occurring on the network [6]. A complete network IPS solution also has the capability to enforce traditional static firewall rules and administrator-defined whitelists and blacklists. Though IPS devices are the most resource intensive, they are still relatively high-performing due to the latest processors, software, and hardware advancements. IPS may be distributed and hardware based [7, 8, 9, 10].

Today two categories of IPS exist: Network-based Intrusion Prevention and Host-based Intrusion Prevention. Network IPS monitors from a network segment level, and can detect and prevent both internal and external attacks. Network IPS devices separate networks in much the same fashion as firewalls. Host IPS software runs directly on workstations and servers detects and prevents threats aimed at the local host. In both cases, attack recognition is usually accomplished via two primary methods of IDS: known-attack detection, and anomalous behavior detection. This paper focuses on Cobrador Bouncer IPS which is an implementation of a network IPS.

The rest of the paper is organized as follows: section 2 presents the system architecture. Section 3 describes Bouncer Intrusion Prevention System concepts. Section 4 points out some of the implementation details. Section 5 describes Bouncer as a proactive honeypot. Finally, section 6 concludes the paper.

2. SYSTEM ARCHITECTURE

Bouncer IPS is a multimodular system. For every function it has component that is designed and specialized for some specific function. Bouncer IPS includes the following components:

- Bouncer Defence Unit (BDU),
- Bouncer Control Unit,
- Bouncer Report Unit (BCU),
- Intelligence Plug-In,

- Alarm Center Plug-In,
- Bouncer Shield Plug-In,
- Update Manager Plug-In, and
- Bouncer Inter-connection Channel (BIC).

The **Bouncer Defense Unit** (BDU) is the core of the intrusion prevention system. Its defined policies determine the level of prevention protection. The BDU is absolutely transparent – it does not affect network traffic – and can be deployed in different deployment methods. It can also be placed on multiple network segments such as the perimeter, *DMZ* and so forth. The BDU can be either set up straightaway using the default set of policies, or deployed after customizing the policies according to the customer's requirements.

The **Bouncer Control Unit (**BCU) is an intuitive and easy-to-use control center. By selecting a BDU from the console, the security operator can set up, monitor traffic, and query logs for all the BDUs in the system. All the communication between the Bouncer and the BCU is through transparent protocol (not TCP/IP), so as to maximize end-to-end security.

The **Bouncer Reporting Unit** (BRU) provides advanced drilldown capabilities integrated with a Crystal Reports engine. The user-friendly report format provides comprehensive information for managers on both operational and tactical levels.

The **Bouncer Intelligence Center Plug-In** is responsible for aggregating attacker information during the attack. Furthermore, it supports adaptive context building and triggering of various responses. The intelligence plug-in is installed as a separate device for central intelligence gathering. The amount and type of target data collected is defined in the BDU security policies. In addition, the intelligence plug-in provides high quality graphic representations of both the attackers' activity and the scale of the attack.

The **Alarm Center Plug-In** is responsible for consolidating and distributing alarms to an array of alarm devices (mobile phones, pagers, email accounts etc.). It is installed as a separate device that consolidates alarms from different BDUs and disseminates alarm information between the BCU, BDUs, and designated personnel.

The **Bouncer Shield Plug-In** is responsible for updating and maintaining information of the current most suspicious targets. This information is obtained from reliable industry sources.

The **Update Manager Plug-In** manages the Bouncer system updates such as versions, hot fixes, patterns and security related information for both the BCU and the BDUs.

Bouncer Inter-Connection Channels (BICs) provide seamless connections between the Bouncer IPS components (BDU, BCU, etc.). The main reason for using multiple channels is to maintain reliable separation so that online activities are not disrupted with data probing or data distribution.

The default channels are:

- *Bouncer Control Channel*: Transparently carries control commands from the control unit to any of the managed BDUs without interfering with organizational processes. In addition, this channel is used for context distribution and dynamic group sharing.
- *Bouncer Data Channel*: Transparently carries off-line data such as report queries, history probing and any other drilldown data view you would like to see.

- *Bouncer Virtual Channel*: Plug-in channels for communicating with external systems such as syslog or storage devices.

Bouncer IPS enables duplicating channels for maintaining evidence. All the chanels are using non-standard protocols and additionally encrypted for increased security.

3. BOUNCER IPS CONCEPTS

3.1. Modals

Modals are abstract objects aimed at performing a variety of security operations such as selecting IP packets, choosing patterns, faking responses, defragmentation, monitoring, protocol analysis and so forth. Modals contain operational methods but do not embed security data. In fact, the modal itself is used to perform different operations with different data and different parameters. A modal can be dynamically updated without reinstalling or stopping the BDU.

3.2. Bricks

Bricks are specific implementations of the modals. Bricks are the building blocks of the Bouncer security policy. Brick data can be modified automatically, on the fly, with information gathered in real-time.

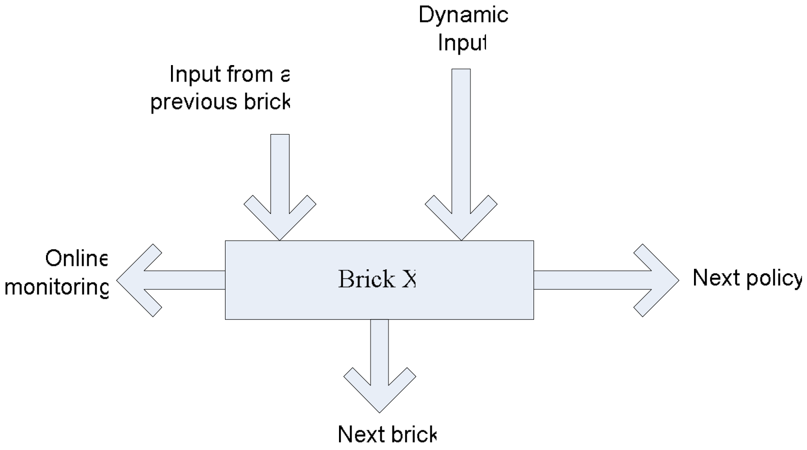


Figure 1: The Brick Method of Operation

Bricks - like Modals - can be added, updated and distributed without reinstalling or stopping the Bouncer activity. Bricks support a variety of inputs as shown in Figure 1. Inputs can result from previous inspections or from dynamic lists of values. A brick will choose a course of action according to its embedded modal. This course determines the inspection flow within a single policy and between policy chains.

3.3. Policies

Policies are chains of bricks that are executed by the BDU engine. When you define a policy you set up an inspection and operation flow composed of predefined bricks. Bricks are applied as they are ordered inside the policy (Figure 2) and the last brisk is usually the one that defines the action that will be taken with the packet.

Different inspection policy types use different types of bricks:

- Packet-level inspection policies
- Protocol-level inspection policies
- Application-level inspection policies
- Bandwidth-level inspection policies
- Reconnaissance policies

You can add logging capabilities to a policy by adding logging bricks.

Bouncer policies are dynamic and can be created before the target group is defined. The Security Manager can then define an operative profile for that particular policy. Policies are executed according to their priority and level of inspection. The Bouncer provides a visual display of the execution plan so the security manager knows in advance the chain of operations involved in each scenario. This feature provides a wealth of information that increases the effectiveness of the inspection process. Policies, like bricks, can be added to, updated and distributed without reinstalling or stopping Bouncer activity. This option consolidates management and helps create unified security policies, which are distributed to all protected locations.

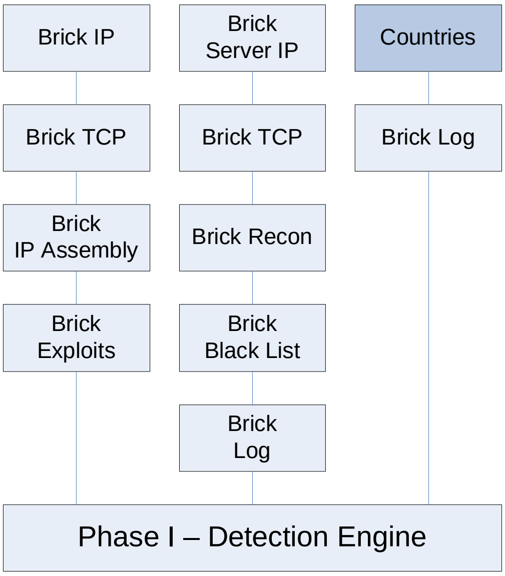


Figure 2: Policy Brick Flow

Within each level, policies are executed according to priority level set to them. The unique Matrix view shown in Figure 3 allows you to see a visual presentation of the system workflow (security flow). This way, it is possible to make very good prediction of a package's way through the policy chains based on different scenarios that are created. This feature is rare in today's security systems and is extremely useful for the security personnel.

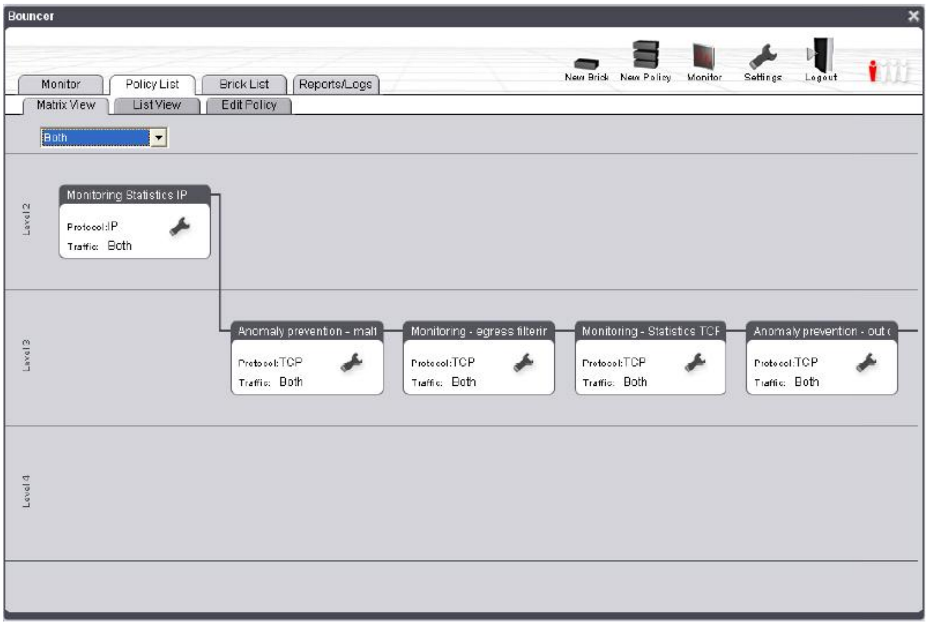


Figure 3: Security Flow

3.4. Adaptive Context Containers (ACCs)

Adaptive Contexts Containers (ACCs) are created online. They contain cross policy groups for example, a list of the most active attackers with the same profile. These contexts may be used as dynamic selectors for any of the Bouncer bricks. ACCs may be distributed or even created in a central location providing cross-site intelligence gathering. ACCs are saved in history logs. The Bouncer provides drilldown and cross-reference methods that enable target tracing activity.

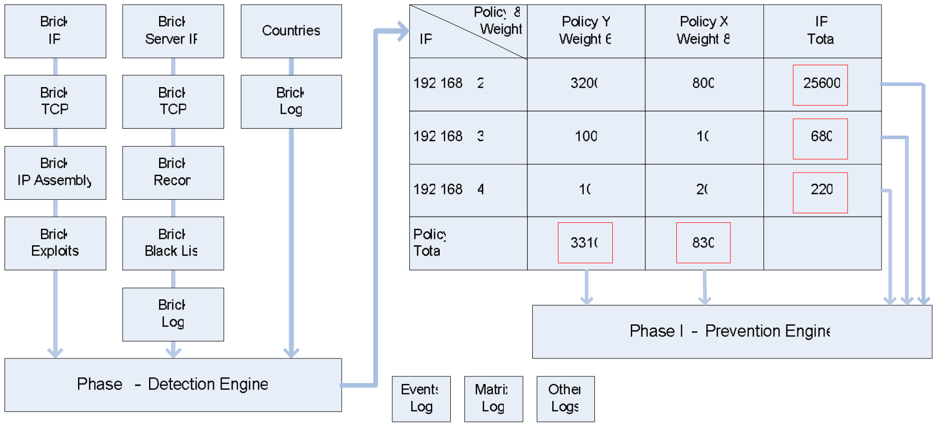
3.5. Target Activity Inspection Matrix (TAIM)

The Target Activity Inspection Matrix (TAIM) supports attack prevention while avoiding false positives. The basic concept is building a dynamic matrix that follows cross-policy target activity with reference to global contexts (intelligence). The matrix is used as the basis for network traffic filtering.

TAIM preventive decisions are based on making a cross-reference to the attack profile instead of using flat detection (single policy detection).

This is done in two steps (Figure 4):

1. The first step involves building the matrix.
2. The second step involves making a preventive decision based on this matrix.



Policy & Weight / IF	Policy Y Weight 6	Policy X Weight 8	IF Tota
192 168 2	320(	800	25600
192 168 3	100	1(	680
192 168 4	1(	2(	220
Policy Tota	331(	830	

Figure 4: Example of TAIM

From a usability point of view, the TAIM introduces a new generation of practical monitoring. By showing the attack flow itself (instead of many events) the Security Manager gains a better understanding of the security state at any given moment.

4. IMPLEMENTATION NOTES

With cyber threats growing constantly, preserving a sufficient level of security means you must utilize advanced technologies to protect your assets. The Bouncer IPS is a very efficient intrusion prevention system. Unfortunately, there is no hit-and-win solution that will keep your assets protected without a well planned security preservation working plan.

The recommended steps for implementing the Bouncer IPS are:

STEP 1. Define the deployment strategy and security objectives,
STEP 2. Define the security baseline to achieve these objectives, and
STEP 3. Define a security-in-action plan to preserve these objectives.

4.1. Bouncer IPS Deployment

The Bouncer IPS delivers unprecedented flexibility in IPS deployment. It supports versatile deployment options and enables integration in a wide range of network architectures.

The Bouncer IPS supports the following deployment configurations:

- SPAN configuration (Passive Sniffer Mode),
- Tap configuration,
- Inline configuration (Active Gateway Mode), and
- Virtual IPS.

4.1.1. SPAN Configuration (Passive Sniffer Mode)

Hub ports or SPAN ports from one or more network switches can be connected to the BDU detection ports. Response actions, such as resetting a TCP connection, can be injected by the BDU using the same port.

4.1.2. Tap Configuration

Network communication is monitored in both directions by a full-duplex Ethernet network link. By fully capturing all the traffic on a link, a clearer understanding of the source and nature of the network attack can be delivered. This provides the detailed information needed to thwart attacks. This full duplex monitoring capability allows the Bouncer system to maintain complete state information. Response actions include firewall configuration or initiating TCP reset through dedicated response ports.

4.1.3. Inline Configuration (Active Gateway Mode)

Sensors prevent network attacks by dropping malicious traffic in realtime. They are situated on the data path, with active traffic passing through them. Preventive actions can be at a highly granular level, including automated dropping of DoS traffic intended for specific Web servers. Prevention speed and high availability enable IPS deployment in mission-critical environments.

4.1.4 Virtual IPS

Sensors support the innovative and powerful concept of a Virtual IPS. Virtual IPS describes the capability to segment a sensor into a large number of virtual sensors that can be completely customized with a granular security policy. This includes individualized attack selection and associated response actions. A Virtual IPS can be defined based on a block of IP addresses, one or more VLAN tags, or by specific port or ports on a sensor.

4.2. Choosing the Deployment Mode

The first step of setting up the Cobrador Bouncer System on a network is to decide on a deployment mode. The Bouncer IPS is complementary to existing IDS and Firewalls. It is fully transparent at level 2 and does not require any adaptations. This means it can be incorporated in different deployment modes in existing systems.

Bouncer Placement

You can place the Bouncer system either in front of your firewall, behind it, or anywhere on your network. You should choose the location for your Bouncer system based on your existing network hardware and the network you want to protect. The most commonly used deployment modes and their primary advantages and disadvantages are described in the following sections.

Bouncer Deployment Modes

You can deploy the Bouncer Defense Unit (BDU) in one of the following modes:

- Active gateway: This mode takes full advantage of IPS attack prevention capabilities and multi-layer detection mechanisms
- Passive sniffer: To use Bouncer as an advance network probe for collecting evidence, monitoring your network and logging traffic deploy it in passive mode. If the bouncer is attached to a network switch, you must configure the switch to mirror all traffic to that port.
- Hybrid mode: A combination of two or more BDUs, deployed in different modes, working together in order to collect evidence and prevent intrusions.

You can deploy these BDUs on different segments of the protected network while using a single management console (BCU).

The following examples will help you determine which deployment mode to use for your network.

Active Gateway Mode

Active Gateway Mode is shown in Figure 5. Both BDUs shown are configured as inline filtering all the network traffic that passes through. The BDU protecting the primeter has security policies defined for protecting the whole network. The second one is configured particulary to protect the database DMZ, and it covers specific kind of threats depending on the datababase management software in use.

Usage examples:

- Preventing intrusions and probing targets
- Preventive Honey-pot
- Network level prevention

Advantages:

- Reliable response and prevention of attacks.
- Simple transparent deployment and management – once the BDUs are configured, only thing needed is to connect them onto the network. Once connected and started, there is no need to disconnect or stop them because every change in the configuration can be made on-line.
- No changes needed to routing tables or network equipment – the Bouncer IPS is virtually invisible for any network device, it has no IP or detectable MAC address, its deployment doesn't need any additional setup of the existing network.
- Transfers non-IP traffic.

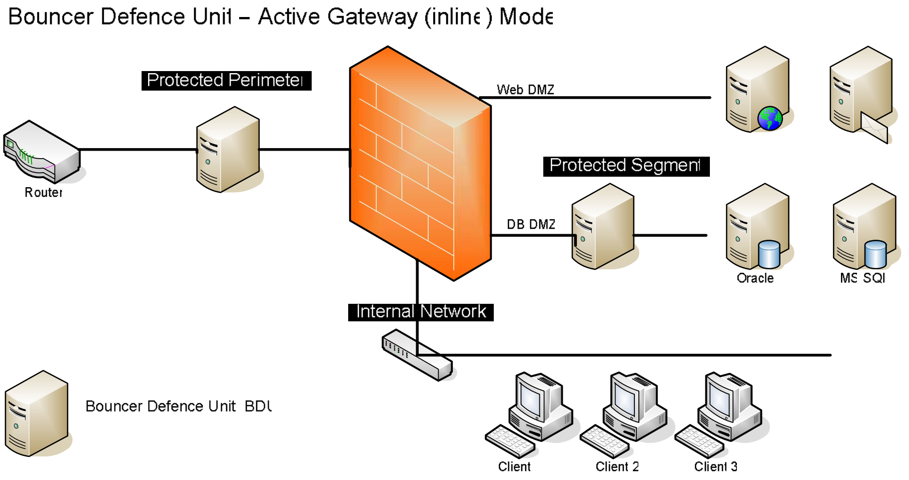


Figure 5: Active gateway mode (transparent) perimeter and DMZ deployment

Disadvantage:

In this mode all traffic actually flows "through" the BDU. The Bouncer is a software IPS implementation and if the network traffic is very intense, appropriate hardware should be used. If high availability configuration is not used, the BDU might become another point of failure.

Passive Sniffer Mode

Passive Sniffer Mode is shown in Figure 6. The BDUs are configured as SPAN devices so they are just monitoring the network traffic. Similar to the active gateway mode, in this mode the BDU protecting the perimeter monitors the activities that can endanger the network as a whole. The second one focuses on the specific threats for the protected segment. Combining the data collected by both of the BDUs, very complex analysis can be made.

Usage examples:

- Probing mode: collecting evidence and suspicious activity
- Honey-pot simulation
- Network traffic interception and optimization
- Learning and testing

Advantages:

- Seamless replacement of current IDS – in this mode the Bouncer actually does not interfere with the traffic. It only creates logs for further analysis.
- Does not create an additional point of failure – BDUs are inspecting mirrored traffic, so the actual traffic flows without any delay.

- Minimal network changes required - must use a HUB or a SPAN port on a switch.
- Fully utilizes the advance Bouncer policy logic to log and intercept traffic.

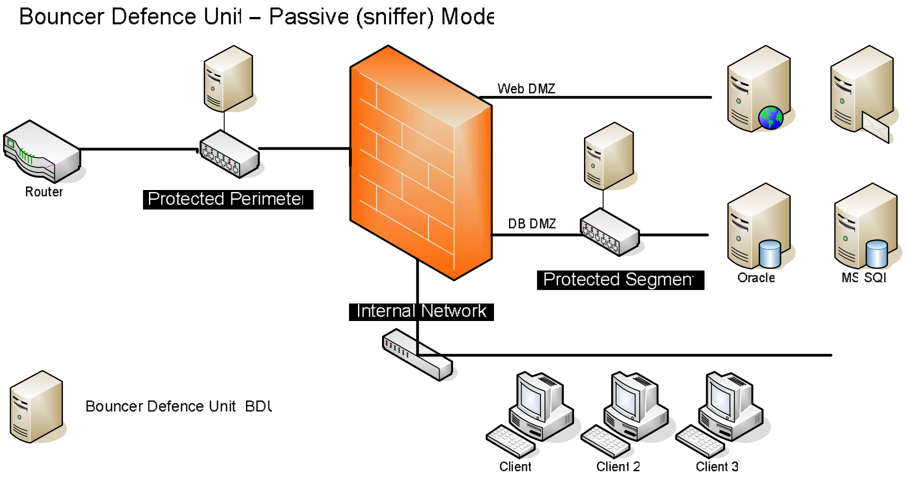


Figure 6: Passive (sniffer) mode (Transparent) perimeter & DMZ deployment

Disadvantages:

- Limited prevention capabilities – in this mode BDUs are not able to make interventions on the traffic.

Hybrid Mode

Hybrid Mode is shown in Figure 7. This mode combines span and inline configuration. The BDU deployed at the primeter is monitoring all the network trafic, mainly for collecting evidence, while the BDUs protecting the segments shown are preventing attacks. Inline configured BDUs can be configured to generate fake or slow responses in order to confuse the attacker and slow down the attack. In that case, the BDU on the perimeter can be provided additional time to gather more informatin on the attacker and the attack itself.

Usage examples:

- Probe mode: collecting evidence and suspicious activity from one segment while preventing attacks on the other.
- Active honey-pot
- Network traffic interception and prevention

Advantages:

- Seamless replacement of current IDS.
- Does not create an additional point of failure.

- Minimal network changes required.
- Fully utilizes the advance Bouncer policy logic-to-log, and intercept traffic.
- Combines prevention with evidence collection.

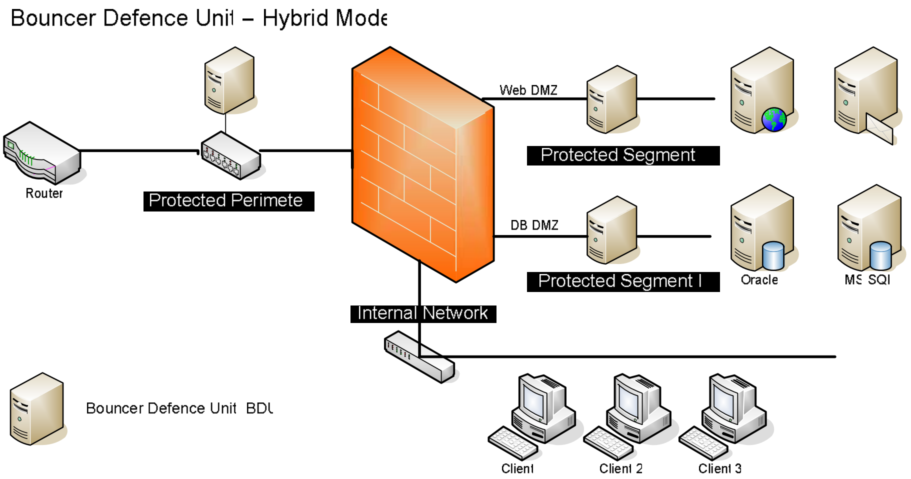


Figure 7: Hybrid mode (Transparent) perimeter and DMZ deployment

Shortly presented, all of the deployment modes are shown in the next table:

Table 1: Overview of The Bouncer’s deployment modes

Configuration mode	Advantages	Disadvantages	Use
Active gateway	Reliable attack response and prevention, simple management and integration within existing networks	If inappropriate hardware is used, possible point of failure.	Preventing intrusion and probing targets, network level protection, preventive Honey-pot
Passive sniffer	Seamless replacement of the current IDS, advanced logic to log and intercept traffic	Limited prevention capabilities	Collecting evidence and suspicious activity, Honey-pot simulation, learning and testing,
Hybrid	Cobmines prevention with evidence collecting	If inappropriate hardware is used, possible point of failure	collecting evidence and suspicious activity from one segment while preventing attacks on the other, active Honey-pot

5. CASE STUDY – THE BOUNCER AS A PROACTIVE HONEYPOT

The Bouncer is the first intrusion prevention system (IPS) that can effectively and easily be deployed as an active honeypot. The main reason is that unlike traditional intrusion prevention and intrusion detection systems it is able to easily manipulate and divert massive amounts of malicious activity.

The Bouncer as a Honeypot

A honeypot is a security resource whose value lies in actually being probed, attacked, or compromised. Whatever resource we designate as the honeypot, our expectations and goals are to have the system probed, attacked and potentially exploited. In this case we use the Bouncer as a high-interaction active honey-pot. This means that, the honeypot computer is running a full service scheme and dedicated applications.

The Bouncer system objectives as a honeypot are:

- Evidence Probing: Acting as an evidence probe.
- Traffic monitoring: Traffic shaping and statistical analysis.
- Counter-intelligence: Real-time intelligence gathering on the attacker and the attacks.
- Analysis and reporting: Providing comprehensive and easy to understand outputs.

Cyber security is an ongoing process influenced by many factors. While some of these factors are internal and under your local supervision, many of them are external and hard to evaluate. The BDU deployed as an active honeypot, provides an excellent security measure, enabling you to follow the number of attacks, method types, and attacker origins, as well as estimate the level of threat to which your protected site is exposed. Furthermore, it allows you to take these inputs into consideration for the purpose of practical prevention.

6. CONCLUSION

Cyber security is an ongoing process influenced by many factors. While some of these factors are internal and under direct local supervision, many of them are external and hard to evaluate. Current security products are based on policies that are predefined by the security team. Each policy specifies the static target group, service, patterns, and set of operations.

Bouncer profile-based policies replace a static group with a dynamic profile, dynamically generating the rule group according to the state of security at any given moment. The Bouncer modifies the data according to the state of security, so you don't need to know in advance who your enemies are. This allows the Bouncer IPS to focus on suspicious packets or streams while minimizing the interaction with good traffic.

Most IDS technologies rely on single-policy detection with each policy acting as an independent decision maker: Forward or Block. Although this is good enough for detection, the real challenge of intrusion prevention lies in the handling of unclear situations, suspicious but not conclusively malicious traffic. The Bouncer solution provides a Target Activity Inspection Matrix (TAIM) that follows target traffic until it verifies that it is harmless. This procedure ensures a low rate of false positives with a minimal effect on normal traffic.

The BDU deployed as an active honeypot, provides an excellent security measure, enabling you to follow the number of attacks, method types, and attacker origins, as well as estimate the level of threat to which your protected site is exposed. Furthermore, it allows you to take these inputs into consideration for the purpose of practical prevention.

Many security products provide an option for tracking down attacker information such as IP addresses. Experts then run probing tools on this information. Using this method creates the following problems:

- Collecting (outdated) off-line information can damage the decision making process.
- Information flooding without the means of incorporating this information into the real-time decision making process.
- Skilled information analysis is usually not available in-house, which means the added cost of consultants.

In addressing these common problems, Bouncer's preventive intelligence implements accurate online intelligence gathering while the attacker is in action.

Usage of the Bouncer IPS had shown us new threats and made us more informed about the number of attacks and ways how our network was attacked.

7. REFERENCES

[1] CSI/FBI, “Computer Crime and Security Survey 2004“, available at the following address: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[2] Baumrucker, C., Burton, J., Dentler, S. et al, *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*, Syngress Publishing, 2003.

[3] Endorf, C., Schultz, E., Mellander, J., *Intrusion Detection & Prevention*, McGraw-Hill 2004.

[4] “Technical Overview of The Bouncer“, http://www.cobrador.net/docs/whitepaper.pdf

[5] Barkett, M., “Intrusion Prevention Systems“, http://www.nfr.com/resource/downloads/SentivistIPS-WP.pdf

[6] Xinidis, K., Anagnostakis, K.G., and Markatos, E.P., “Design and implementation of a high performance network intrusion prevention system“, *Proceedings of the 20th International Information Security Conference (SEC 2005)*, Makuhari-Messe, Chiba, Japan, May 30 - June 1, 2005.

[7] Sproull, T., and Lockwood, J., “Wide-area hardware-accelerated intrusion prevention systems (WHIPS)“, *Proceedings of the International Working Conference on Active Networking (IWAN)*, Lawrence, Kansas, USA, October 27 – 29, 2004.

[8] Sarang, D., Praveen, K., Sproull, T.S., and Lockwood, J.W., “Deep packet inspection using parallel bloom filters“, *IEEE Micro*, Vol. 24, No. 1, Jan. 2004., pp. 52-61.

[9] Schuehler, D.V., and Moscola, J., and Lockwood, J.W., “Architecture for a hardware-based, TCP/IP content-processing system“, *IEEE Micro*, Vol. 24, No. 1, Jan. 2004., pp. 62-69.

[10] Song, H., and Lockwood, J.W., “Efficient packet classification for network intrusion detection using FPGA“, *Proceedings of the International Symposium on Field-Programmable Gate Arrays (FPGA'05)*, Monterey, California, Feb 20-22, 2005.