Towers Net Defender - The New Generation Intrusion Prevention and Detection System

Preface

Towers Net Defender (**TND**) is system for detection and prevention of cyber attack (*Intrusion prevention system - IPS, Intrusion detection System - IDS*). **Towers Net Defender** monitors network and/or system activities for malicious activities, timely identifies them, blocks/stops it and reports about successfully defended attack (generates *Certificate of Successful Defence*), also registers and informs other servers about attacks and records all significant events in the monthly report for user.

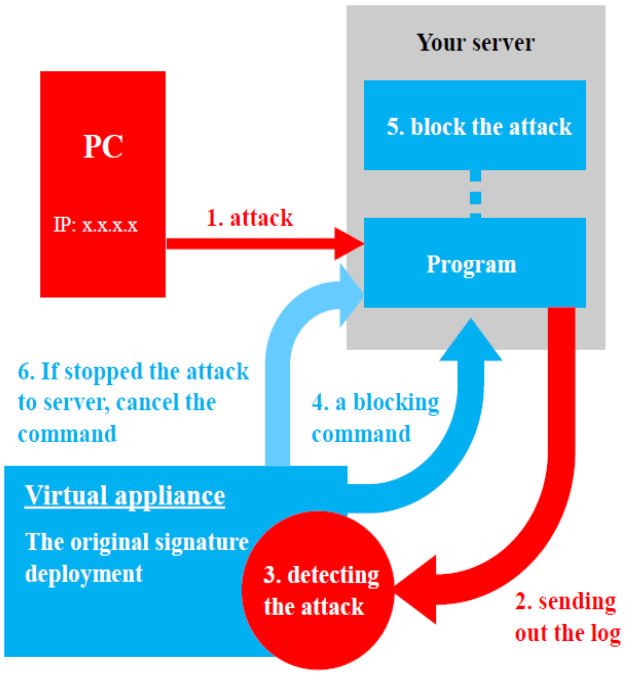
Towers Net Defender Features

- ***Neutralize*** operation of detected malicious packages of information,
- ***Generates*** an alarm (Certificate of Succesfull Defense),
- ***Recognizes*** the nature of unknown malicious attacks (zero day attack) and performs additional checks,
- ***Reset*** the connection,
- ***Block*** traffic from IP address which generates the attack,
- ***Generate*** reports on threats and attacks.

Towers Net Defender – Specifications and Implementation

- ***Agent type, Local NBA IPS class*** - Towers Net Defender is an agent type of IDPS. TND AGENT PROGRAM is activated on the defended server.
- ***Monitoring all log files*** - TND Server is monitoring, in real time, all the log files (Access log, Error log and Sys log) trough an agent program.
- ***Continuously updating of known attacks database*** - TND server has complete database of all known attacks. TND server compares potential attacks in real time with all attacks from the TND database. Every attack is blocked by TND server through an agent program. The database of all known attacks and new malicious software is continuously improving.
- ***White list*** - Client can prepare a safety (white) list of IP addresses, for open access, without checking (service IP addresses, internal IP addresses from the safe segment of the network and similar).
- ***Optimal and efficient reporting*** - TND server sends alarm information (Certificate of Successful Defense) for every blocked attack. Client will receive a monthly report about all important events and attacks to his system.
- ***Very low server capacity usage*** - The maximum usage of server and processor resources is less than 1% , beside that consumption of other server resources is very small (CPU usage, Memory, Power consumption, Network capacity).

- ***Very high TND resistance*** - It is not possible to attack to the agent program or other elements of TND IPS system.



Picture 1. Graf of TND processes functionality.

1. It uses UDP complement port,
2. The log sending out is sys log, access log (Apache) and error log (Apache),
3. Detection of attack,
4. Blocking comand,
5. Stoping the attack,
6. Cancelling the command.

Characteristics of TND service

- **Very small consumption of all server resources (CPU Usage, Memory, Power supply) even during active detection and defense.**
- **Conventional products consume a huge server's resources during detection of the attack,**
- **TND system saves server resources using principle of virtual machine. During defense the agent program only executes the blocking command for any unauthorized access.**
- **Very Cost Effective IDPS - no need for additional costs of training, administration, hardware and maintenance.**

Technical Specification

Services

- **Monitoring 24/7/365,**
- **Detection and prevention of cyber attacks/blocking cyber attacks,**
- **Automatic submission and report of the attack (Certificate of successful defense) to administrator/team safety and response,**
- **Flexible, detailed monthly reporting on all events of importance for the prevention of attacks,**
- **Consultancy regarding safety, risk assessment, periodic assessment of risks status and weaknesses based on the IPS monitoring*,**
- **Advising for optimal actions to minimize risk/weaknesses, fine-tuning of the system in accordance with the actual needs*,**
- **Forensic of IP address,**
- **Engineering support,**
  *** (Note: This item refers to PRIME and EXCLUSIVE services)**

TND detects and blocks:

- ***SYN Floods; DoS/DDoS attacks.***
- ***Zero day attack,***
- ***Advanced persistent threats: Brut-force attack, SQL Injection, Cross-site scriprting (XSS), Root-kit attack,***
- ***And others malwares for backdoor setting…***

Supported Platforms

- **Web servers,**
- **Mail servers,**
- **File servers,**
- **PC servers,**
- **All the servers with Internet access.**

Supported Operating Systems

- **All distributed Linux systems,**
- **Free BSD (all versions),**
- **Opensource BSD (all versions),**
- **Net BSD (all versions),**
- **Solaris 2.7, 2.8, 2.9, 10 i 11,**
- **AIX 5.3, 6.1 i 7.1,**
- **HP-UX 10, 11 i 11i,**
- **Windows 7, 8, Vista, XP i 2000,**
- **Windows Server 2012, 2008 i 2003,**
- **MacOSX 10.**

Availability of VMWare

- **VMWare ESX 3.0, 3.5, 4.0, 5.0 and 5.5 (including CIS check)**

Information for starting the service

- **IP address of the server,**
- **Server's operating system.**

Customer support houres

- **Working days from 9.00AM to 17.00PM, for STANDARD and PRIME services**
- **24/7 for EXCLUSIVE service**

Towers Net Ltd.
Heroja Milana Tepića No.10, Belgrade,
Phone: + 381 (11) 266 24 44,
E-mail: office@towersnet.rs, Web: www.towersnet.rs