

Detection Strategies

Putting together a list of detection strategies and their benefits when put up against each other



netmonastery
active threat defacement

Introduction

netmonastery.com

Attack detection and prevention on the network is a critical requirement for each enterprise. In order to choose from the various detection and prevention options already available a configuration / rating guide is a must have. This is an attempt to bring out the facts that surround technologies available today.

The slide show also discusses Comprehensive Network Attack Prevention also called CNAM, details for the service are introduced after the main slide show



netmonastery
active threat defacement

Scoring

netmonastery.com

Each discussed scenario has been scored on the parameters described below and rated to a maximum of 5 points:

False Positives

The capability of a system to avoid false detection of legitimate users, causing unavailability of services

Active Attacker

The ability of the system to accurately detect attackers that are actively targeting the home network

Prevention

Prevention of malicious packets from entering the home network and effective mitigation of worms

Support + Monitoring

The amount of support for customization, tuning and monitoring that is available

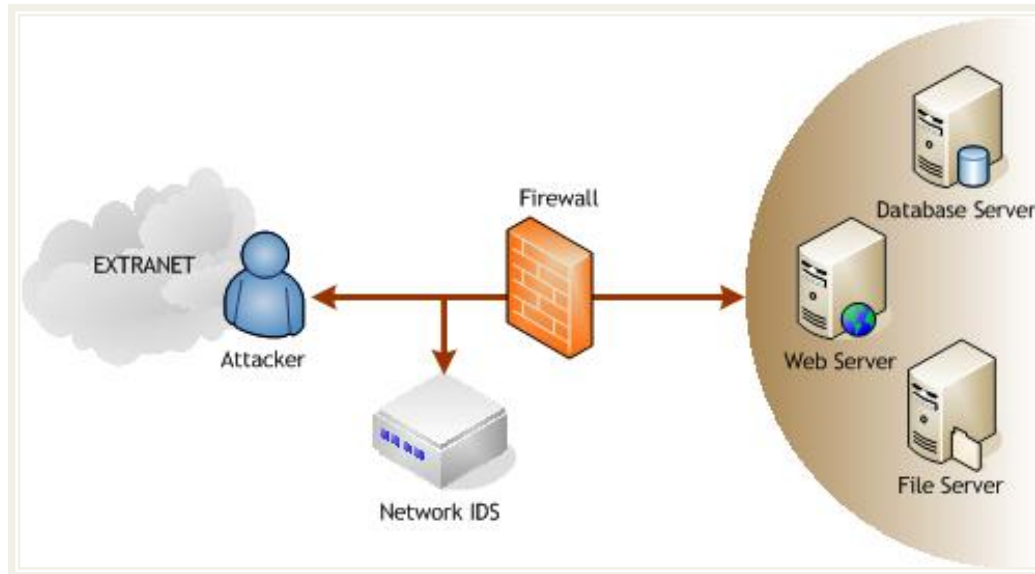
Global Intelligence

The degree of intelligence available based on the daily changing attack perspectives globally



netmonastery
active threat defacement

Deployed IDS



SCORE CARD	
False Positives	2
Active Attacker	2
Prevention	0
Support + Monitoring	2
Global Intelligence	3
TOTAL	9

Positives

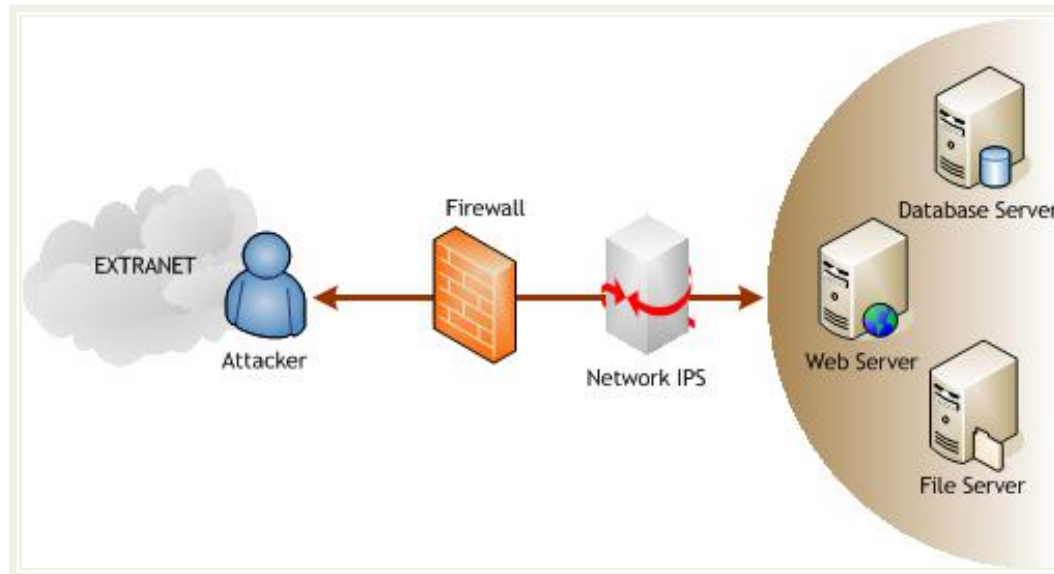
1. Basic detection of attacks
2. Not a point of failure / bottleneck

Negatives

1. High rate of false positives
2. Does not detect active attackers
3. Does not prevent worm outbreaks
4. No attack prevention

Deployed IPS (Non Blocking)

netmonastery.com



SCORE CARD	
False Positives	2
Active Attacker	2
Prevention	0
Support + Monitoring	2
Global Intelligence	3
TOTAL	9

Positives

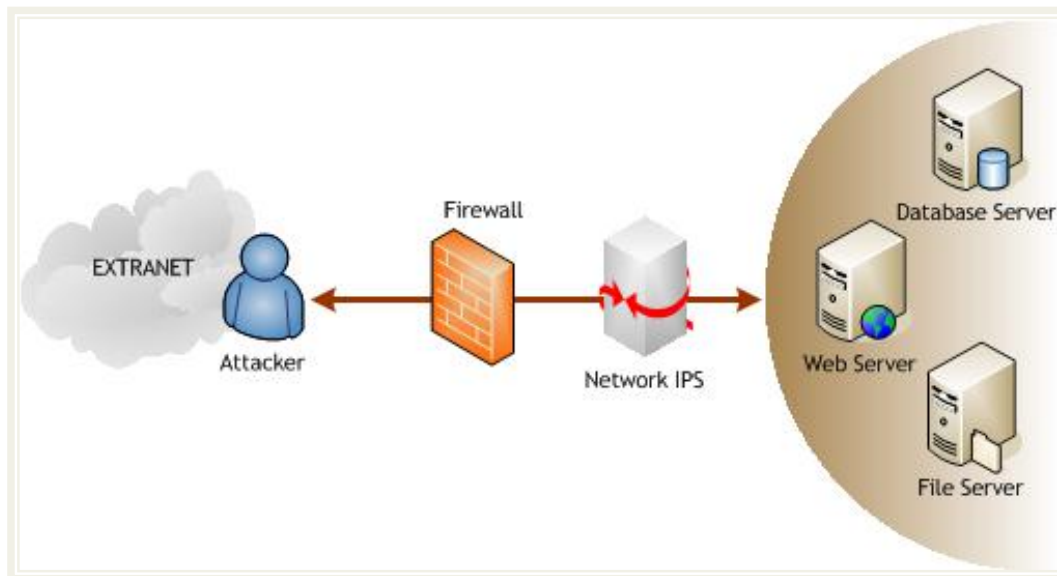
1. Basic detection of attacks
2. Attack prevention in standby

Negatives

1. High rate of false positives
2. Does not detect active attackers
3. Point of failure / bottleneck

Deployed IPS (Blocking)

netmonastery.com



SCORE CARD	
False Positives	2
Active Attacker	2
Prevention	4
Support + Monitoring	2
Global Intelligence	3
TOTAL	13

Positives

1. Prevents attacks in real-time
2. Effective worm mitigation

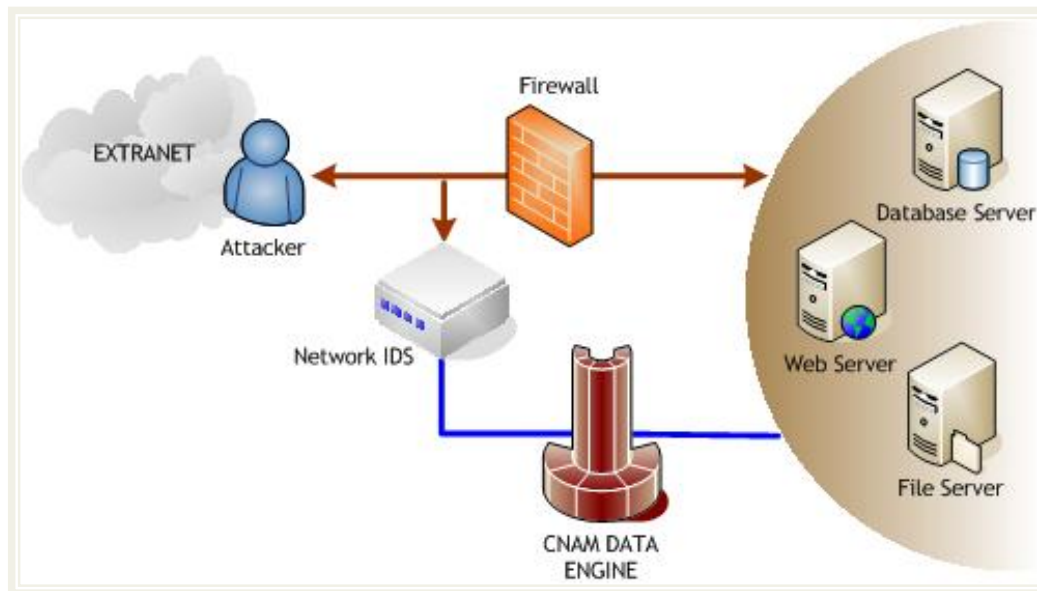
Negatives

1. High rate of false positives, therefore legitimate users denied
2. Does not detect active attackers
3. Requires constant tuning / customization and support
4. Point of failure / bottleneck



Deployed CNAM + IDS

netmonastery.com



SCORE CARD	
False Positives	4
Active Attacker	4
Prevention	3
Support + Monitoring	4
Global Intelligence	4
TOTAL	19

Positives

1. Detection and delayed prevention of active attackers
2. Reduced false positive ratio
3. Global intelligence network
4. 24 x 7 Support and monitoring
5. Not a point of failure / bottleneck

Negatives

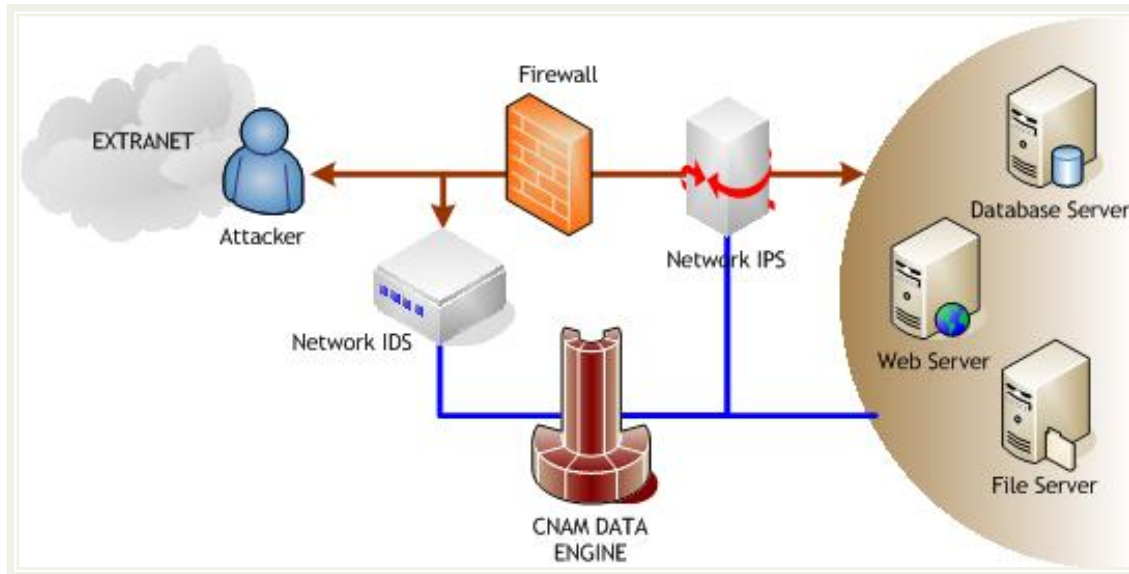
1. Does not prevent worm outbreaks
2. Manual intervention required, may be automated



netmonastery
active threat defacement

CNAM + IDS + IPS (Blocking)

netmonastery.com



False Positives	2
Active Attacker	4
Prevention	4
Support + Monitoring	4
Global Intelligence	4
TOTAL	18

Positives

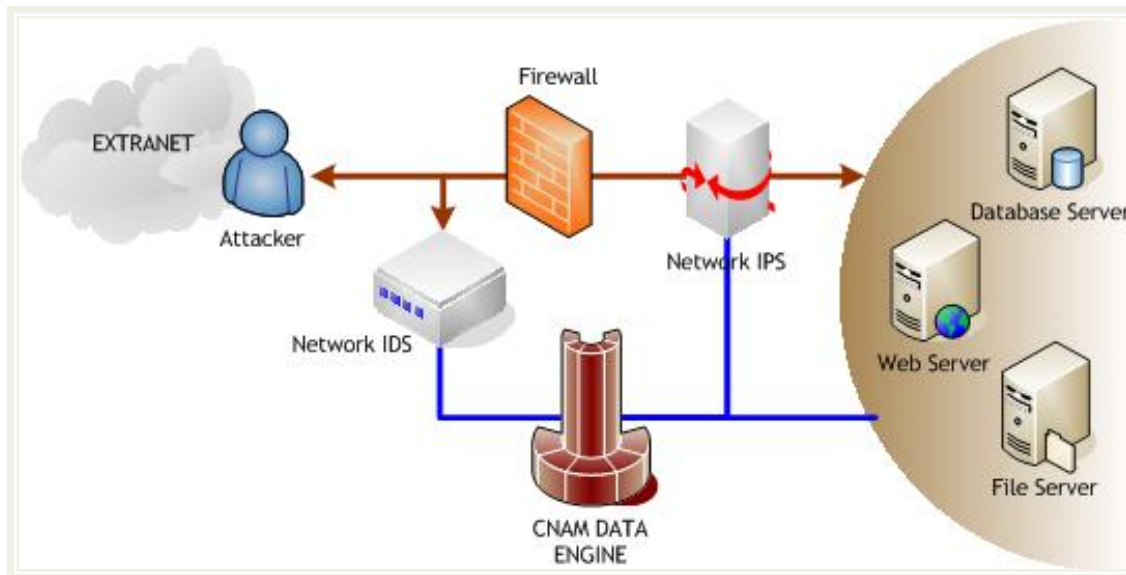
1. Detection and delayed prevention of active attackers
2. Effective worm mitigation
3. Global intelligence network
4. 24 x 7 Support and monitoring

Negatives

1. High rate of false positives, therefore legitimate users denied
2. Manual intervention required, may be automated
3. Point of failure / bottleneck

CNAM + IDS + IPS (Restricted)

netmonastery.com



SCORE CARD

False Positives	4
Active Attacker	4
Prevention	4
Support + Monitoring	4
Global Intelligence	4
TOTAL	20

Positives

1. Detection and delayed prevention of active attackers
2. Effective worm mitigation
3. Reduced false positive ratio
4. Global intelligence network
5. 24 x 7 Support and monitoring

Negatives

1. Manual intervention required, may be automated
2. Point of failure / bottleneck

CNAM – A refresher

netmonastery.com

CNAM is a service provided by NetMonastery, that analyzes events from IDS, IPS and OS logs in real-time and identifies active attacks and attackers. Following are its key features:

- Active correlation and analysis of events generated
- Continuous monitoring / tuning / customization of detection engines
- Individual event support with onsite / offsite incident handling
- Level three escalation and support for mysterious activity analysis
- CNAM Engine and attack monitoring console (GUI) for security monitoring
- Level one and two support for limited firewall management (Support Partner)
- 24 x 7 Monitoring of the security landscape (Support Partner)



netmonastery
active threat defacement