

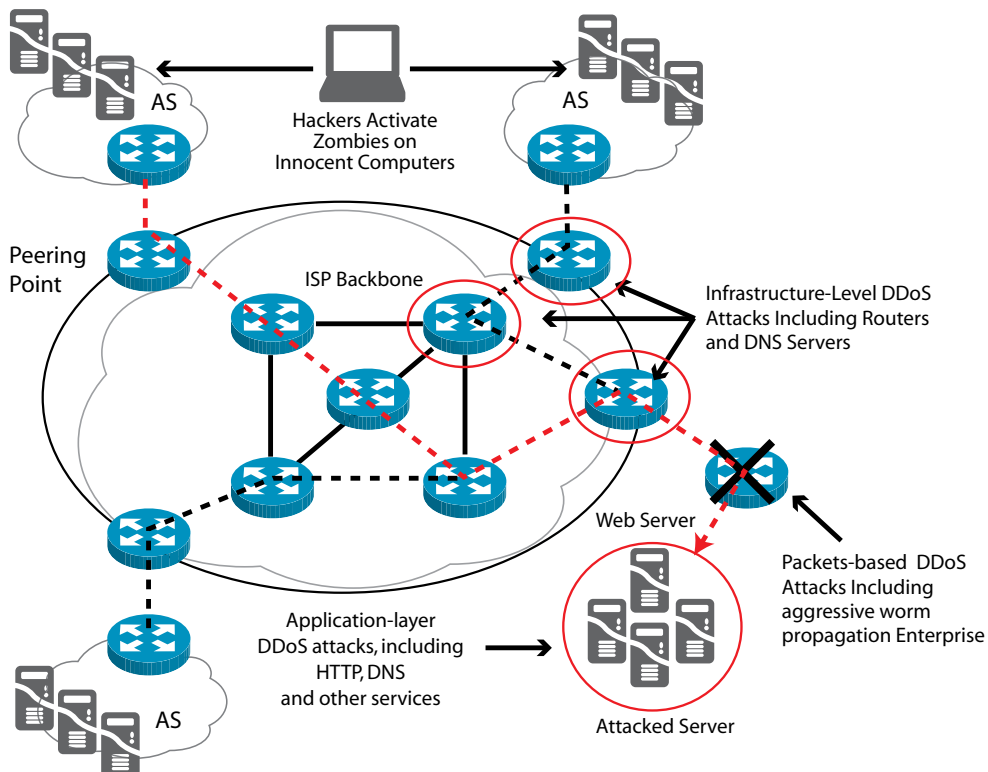


## Cisco Guard Service

Every business transaction should be made precisely, securely and ready to respond to the requirements which become more complicated nowadays. Thus, organizations inquire the best solutions to create business opportunities and enhance the competitive advantages. The solution should operate efficiently as well as maintain the corporate security regarding to reduce risks and system complication. And the key objective is to help reduce cost of business operation.

The Cisco Guard service helps organizations to monitor and detect the presence of DDoS attacks and botnets. Also identifies deviations from "normal" behavior that indicates an attack, allowing detection of attacks that had never been seen before without relying on signature updates to ensure that your business is free from the attacks.

### What is a DDoS Attack?



**Cisco Detector Feature**

- Detects and identifies the sources of DDoS attacks, including massive Botnet attacks.
- Monitors copies of Internet traffic flows entering protected zones, enabling rapid, accurate, and precise detection of all types of attacks
- Uses Cisco’s MVP-based anomaly recognition technology to identify deviations from “normal” behavior that indicates an attack, allowing detection of attacks that had never been seen before without relying on signature updates
- Session State Context is used for recognizing validated session traffic, identifying abusive session attacks and providing an additional protection against malicious activity
- Resides off the critical network path and does not require network device statistics collection that might interfere with network operations while under attacked

**Cisco Guard Feature**

**Performance**

- Only traffic destined for targeted victims is diverted for inspection and cleaning, allowing unaffected traffic to flow unimpeded
- Legitimate traffic passes to its original destination, helping to ensure that transactions are unaffected by attacks

**Attack Coverage**

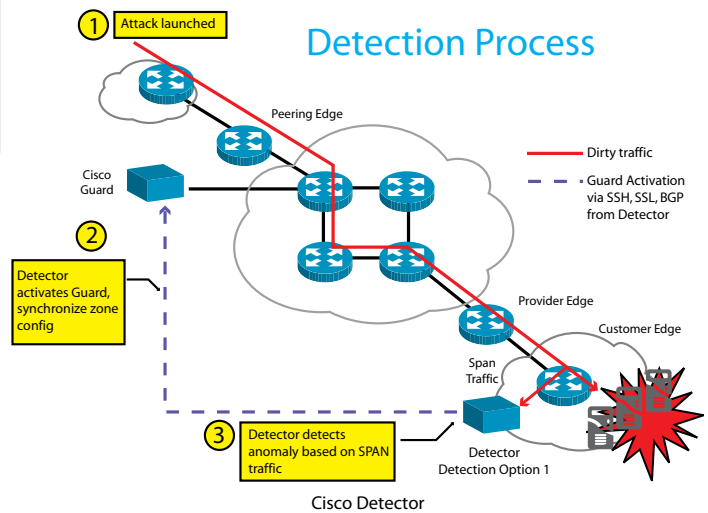
- Highly sophisticated algorithms and traffic analysis enable the Guard to detect and defeat the advanced attacks
- Zombie Killer capabilities allow a single Guard to identify and protect more than 100,000 individual zombies

**Attack Protection**

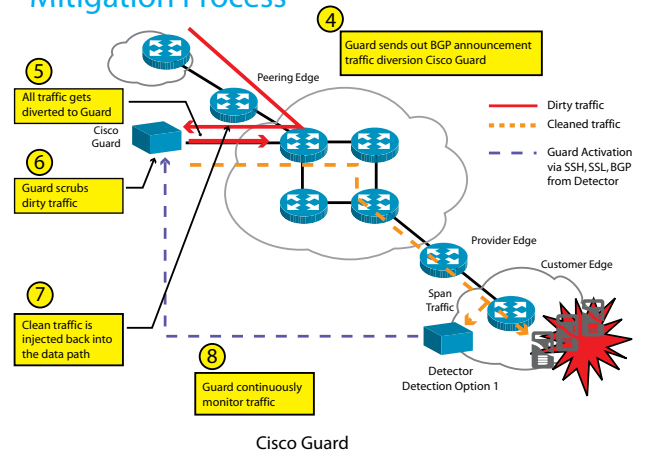
- Enables Random Spoofed attacks protection
- Identifies spoofed that infected to traffic precisely
- Enables Non spoofed Distributed attacks i.e. high volume, massive and morphing botnets
- Enables Non spoofed Client attacks i.e. http half-open

**Monitoring and Report**

- Zone-level views provide a log of events for the selected zone, including attack history, durations, and types, helping the operator anticipate and respond appropriately to future events
- Historical reports provide visual records of attacks and associated responses over time for determining attack patterns.



**Mitigation Process**



**The Solution is suitable for;**

- Organizations who require security on network
- Organizations who do not require to invest in network system (Hardware, Software, License)
- Organizations with few system administrators
- Organizations who require a system administrator who is expert in installing and maintaining the efficient and secured system
- Organizations who require extra security in network system

Remark: The service is available in Bangkok and Vicinity only.

For more information, contact Business Solutions Department at 0 2979 7999  
 Email: consultantksc@ksc.net or use Live Assistant Service at www.ksc.net (Free of charge.)