



DDoS: Anatomy of an Attack A Packet Flow Perspective



Objective

This example follows an attack through the Cisco® Guard DDoS Mitigation Appliance process to explain and simplify the following:

- **Understand the different modes, policies, and filters that are used and created.**
- **Understand the different “show” reports that could be used to explain how the flow of traffic ties in with the protection cycle that is at play in the guard module.**

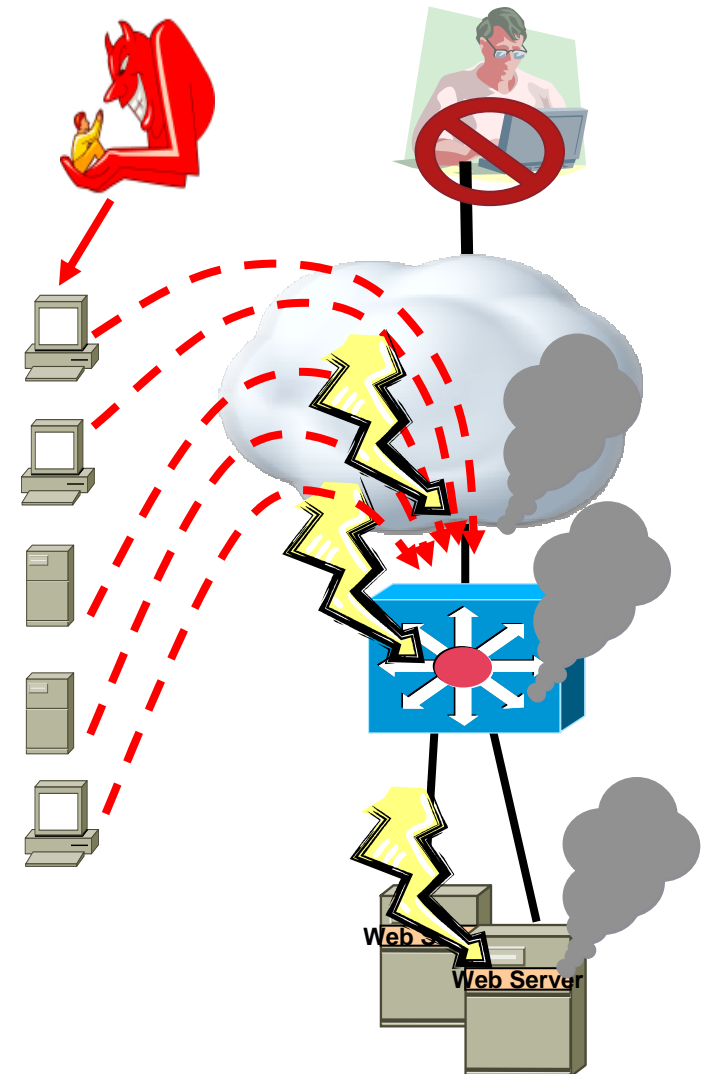
Assumption

- **This example runs through a few simple attack vectors so that a minimal number of policies are triggered, making it easier to explain from a packet flow perspective.**
- **The Cisco® Guard DDoS Mitigation Appliance is in protect mode to begin with. (This example does not include explanations of all the different mechanisms available with the guard.)**

Denial-of-Service Attacks

DoS and DDoS

- Denial-of-service (DoS) attacks are meant to **deny** access to authorized users and **consume** enterprise resources:
 - *Bandwidth*
 - *CPU*
 - *Memory blocks*
- The hacker can use compromised PCs and servers that become zombies or bots to launch the attack (distributed DoS [DDoS]).

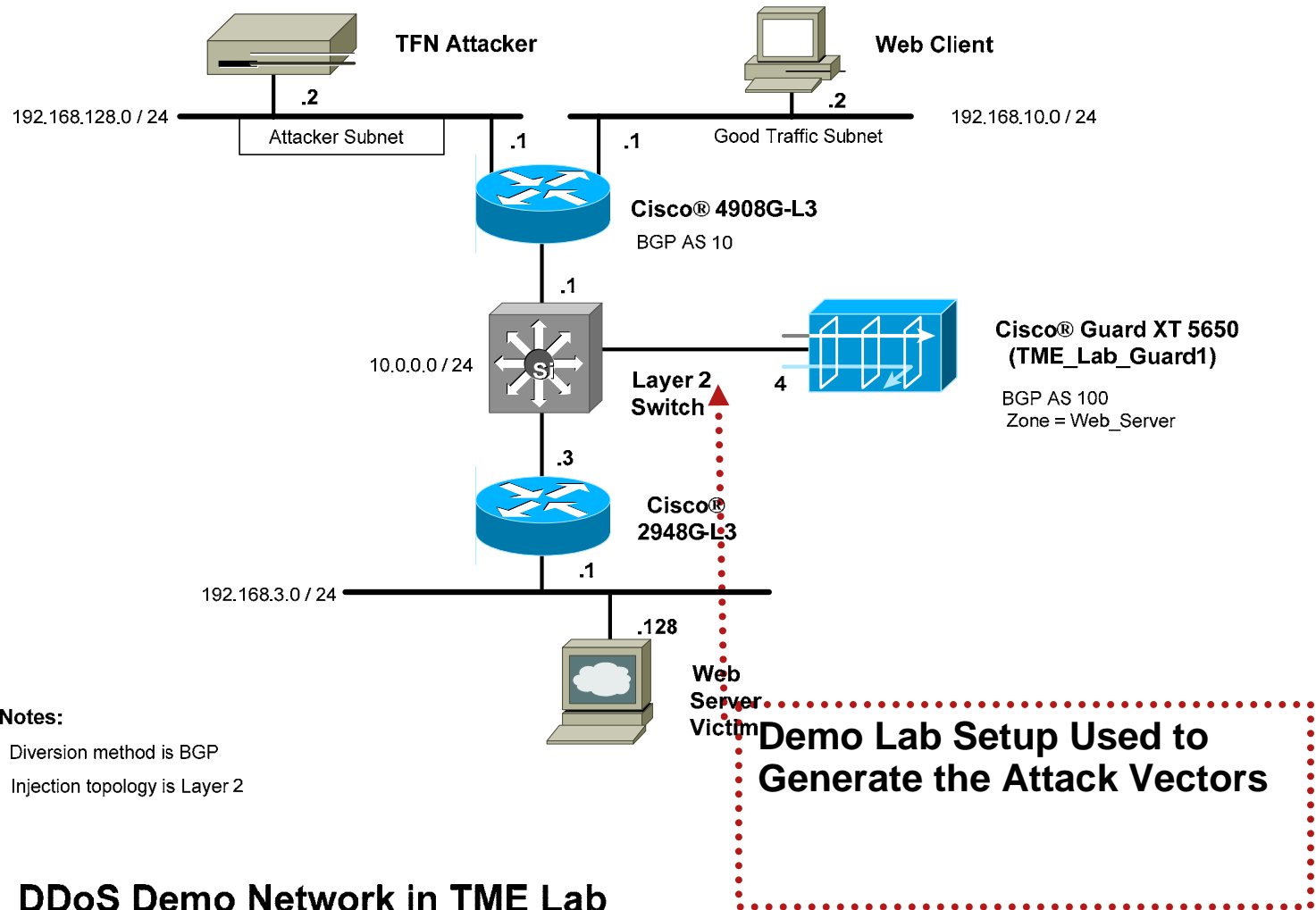


TYP SYN Flood Attack Vector

With the TCP SYN Flood attack, the attacker is hoping to:

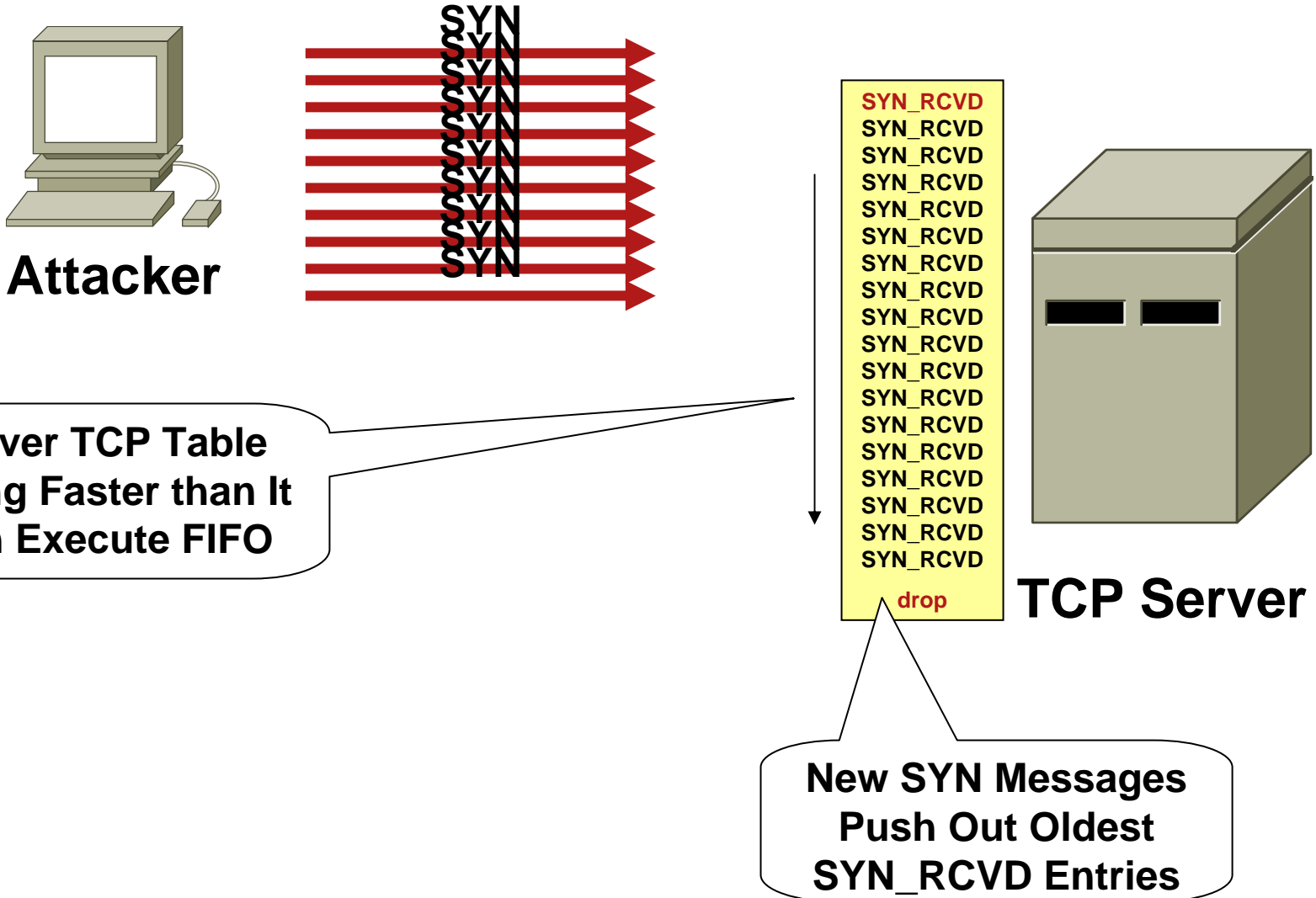
- Fill and overflow the TCP server queue (memory) so that the oldest SYN_RVCD entries are flushed.
- Fill the TCP queue faster than the typical SYN + ACK round-trip time (RTT) so that valid customer SYN_RVCD entries are crowded out.

TYP SYN Flood Attack (Spoofed)

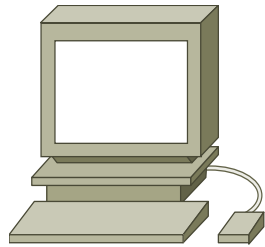


DDoS Demo Network in TME Lab

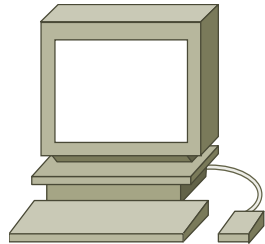
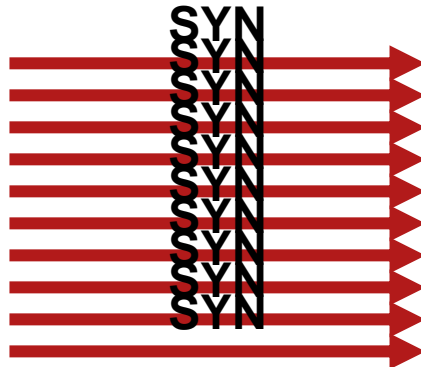
TCP SYN-Flood – Pushing Out the Old Entries



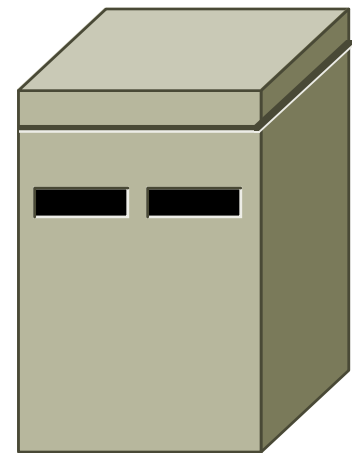
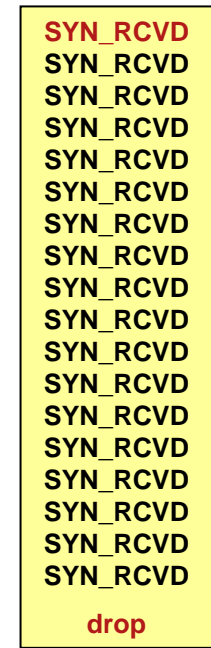
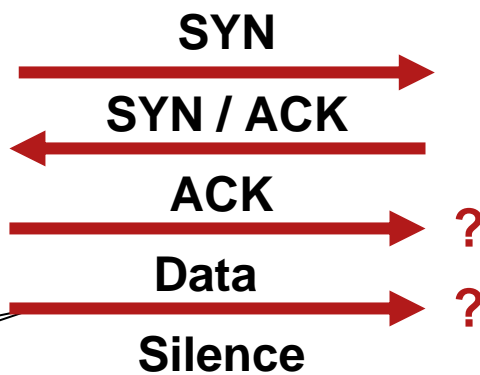
TCP SYN-Flood – SYN_RCVD Gets Pushed



Attacker



Valid User



TCP Server

Valid User Gets to the ACK, but the Server Does Not Set Up

No SYN_RCVD Waiting when the ACK Gets Back

Understanding Policy Types

- The Cisco® Guard DDoS Mitigation Appliance has policy templates that can be used to construct the policy. Policies can even be constructed based on onsite learning.
- There are several policy templates, including:
 - Tcp_services (for non HTTP TCP services)
 - Udp_services (User Datagram Protocol [UDP] services)
 - http (HTTP that flows through port 80)
 - Dns_tcp (DNS-TCP protocol traffic)
 - Tcp_connections (connection characteristics)
 - Tcp_ratio (ratios between different types such as syn vs fin/rst)
 -
 -
 - Other protocols (those not covered or learned explicitly by the guard)

Zone Demo (automatic) - Protected Home > Zone > General

General configuration

Name: Demo

Description:

Operation mode: automatic

Zone Template: GUARD_DEFAULT

Rate: unlimited Burst: unlimited

Attack detection/termination parameters:

Malicious-rate detection threshold: 10.0 pps

Protection-end timer: Never

Filter-rate termination threshold: 2.0 pps

Malicious-rate termination threshold: 50.0 pps

Activation parameters:

Activation interface: Zone name

Activation extent: IP address only

Packet Dump parameters:

Auto Packet Dump: Off

Max. disk space: 2048 MB

Config

	IP	Mask	Type
<input type="checkbox"/>	192.168.3.0	255.255.255.0	REGULAR

Configuration for Zone Default Zone Template that Dictates the Choice (Proxy or No Proxy) Type of Protection. Other Valid Choices are: GUARD_TCP_NO_PROXY GUARD_VOIP

Guard

- Guard Summary
- Protected Zones (1)
 - Demo
- All Zones (4)
 - Demo
 - terry
 - tme
 - Worm

Zone Demo (automatic) - Protected

Home > Zone > Policy Templates

Add service Remove service

Policy Template	State	Min Threshold	Max Services
tcp_services		10.0	5
tcp_services_ns		10.0	3
udp_services		10.0	5
tcp_connections			
dns_udp			
dns_tcp			
http		10.0	
tcp_outgoing			
ip_scan	disabled		
port_scan	disabled		
tcp_not_auth			
fragments			
other_protocols		10.0	5
tcp_ratio			

The Policy Templates that Are Continuously Monitored Based on Traffic Protocol Type

- Guard
- Guard Summary
- Protected Zones (1)
 - Demo
- All Zones (4)
 - Demo
 - terry
 - tme
 - Worm

Zone Demo (automatic) - Protected

Home > Zone > Policy Templates

Add service Remove service

Policy Template	State
tcp_services	
tcp_services_ns	
udp_services	
tcp_connections	
dns_udp	
dns_tcp	
http	
tcp_outgoing	
ip_scan	disabled
port_scan	disabled
tcp_not_auth	
fragments	
other_protocols	
tcp_ratio	

Screen for Select TCP Services; Click to See Details

https://172.25.89.75 - Policy filter - Microsoft...

Policy filter

Policy template: tcp_services

Service: All

Protection level: analysis

Type: — select policy type —

Policy: — select policy name —

State: — select policy state —

Action: — select policy action —

Policies: Current configuration

OK Clear Cancel



GUARD

November 20, 2006 09:22

User name: s
Privileges: dynam

Guard

Guard Summary

Protected Zones (1)

Demo

All Zones (4)

Demo

terry

tme

Worm

one Demo (automatic) - Protected

Home > Zone > Policies

Screen filter:

Path: tcp_services/* /analysis/* /*

Policies: Current configuration

State: All

Device: Guard

Details List the Parameter Used to Analyze the Flow, such as dst_ip, src_ip etc.

Config selection Add service Remove service View Detector

<input type="checkbox"/>	Policy Te...	Service	Level	Type	Key	State	Action	Threshold	Proxy Th...	Thres...	Time...	Fixed	Learning
<input type="checkbox"/>	tcp_services	any	analysis	pkts	dst_ip		to-user-filters	100.0	0.0	0	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	pkts	dst_port		to-user-filters	400.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	pkts	global		to-user-filters	150.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	pkts	src_ip		to-user-filters	200.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	reqs	dst_ip		to-user-filters	100.0	0.0	0	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	reqs	dst_port		to-user-filters	250.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	reqs	global		to-user-filters	150.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	reqs	src_ip		to-user-filters	150.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	syms	dst_ip		to-user-filters	50.0	0.0	0	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	syms	dst_port		to-user-filters	150.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	syms	global		to-user-filters	100.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0
<input type="checkbox"/>	tcp_services	any	analysis	syms	src_ip		to-user-filters	150.0	0.0	-	600	<input checked="" type="checkbox"/>	1.0



```
se@GUARD-conf-zone-Demo>show policies | include tcp_services/any/analysis
```

Policy	State	IStatus	Threshold	Proxy List	Action	Timeout
tcp_services/any/analysis/pkts/dst_ip	act	a-accpt	100.00 -	0	to-user-filters	600
tcp_services/any/analysis/pkts/dst_port	act	a-accpt	400.00 -	0	to-user-filters	600
tcp_services/any/analysis/pkts/global	act	a-accpt	150.00 -	0	to-user-filters	600
tcp_services/any/analysis/pkts/src_ip	act	a-accpt	200.00 -	0	to-user-filters	600
tcp_services/any/analysis/reqs/dst_ip	act	a-accpt	100.00 -	0	to-user-filters	600
tcp_services/any/analysis/reqs/dst_port	act	a-accpt	250.00 -	0	to-user-filters	600
tcp_services/any/analysis/reqs/global	act	a-accpt	150.00 -	0	to-user-filters	600
tcp_services/any/analysis/reqs/src_ip	act	a-accpt	150.00 -	0	to-user-filters	600
tcp_services/any/analysis/syns/dst_ip	act	a-accpt	50.00 -	0	to-user-filters	600
tcp_services/any/analysis/syns/dst_port	act	a-accpt	150.00 -	0	to-user-filters	600
tcp_services/any/analysis/syns/global	act	a-accpt	100.00 -	0	to-user-filters	600
tcp_services/any/analysis/syns/src_ip	act	a-accpt	150.00 -	0	to-user-filters	600

The same set of services when viewed through the CLI commands on the Cisco® Guard DDoS Mitigation Appliance; multiple elements of the same packet are analyzed (packets, registrations, syn messages, etc.) along with `dst_ip`, `src_ip`

All these services listed selectively apply to the traffic flows during the “analysis” mode; that is the first mode the Cisco® Guard DDoS Mitigation Appliance starts in.

- It is important to understand the *action* “to-user-filters”, which specifies traffic to be directed to the user filters *before* going on to the basic mode.
- The filter will live 600 sec (10 min) as long as there is no more activity.



```
Template: GUARD_DEFAULT
Activation-Interface: zone-name-only
Activation-Extent: ip-address-only
Protection-End Timer: forever
Filter-termination filter-rate      threshold: 2.00 pps
Filter-termination zone-malicious-rate threshold: 50.00 pps
Attack-detection zone-malicious-rate threshold: 10.00 pps
RATE: no-limit

SUBNET: 192.168.3.0 255.255.255.0
                pps                bps
Legitimate traffic: 0                0
Malicious traffic: 0                0

There are no dynamic filters
There are no bypass filters
```

Traffic Could Get Directed to the USER FILTERS as They Go Between the Analysis and Basic Modes.

**** USER FILTERS ****

Row	Source IP	Source Mask	Proto	DPort	Frg	Action	Rate	Burst	Units	RxRate(pps)
10	*	255.255.255.255	6	80	no	basic/redirect				0
20	*	255.255.255.255	6	8080	no	basic/redirect				0
30	*	255.255.255.255	6	8000	no	basic/redirect				0
40	*	255.255.255.255	6	8008	no	basic/redirect				0
50	*	255.255.255.255	6	8081	no	basic/redirect				0
60	*	255.255.255.255	6	3128	no	basic/redirect				0
70	*	255.255.255.255	6	53	no	basic/dns-proxy				0
80	*	255.255.255.255	6	25	no	basic/safe-reset				0
90	*	255.255.255.255	6	110	no	basic/safe-reset				0
100	*	255.255.255.255	6	143	no	basic/safe-reset				0
110	*	255.255.255.255	6	6667	no	basic/safe-reset				0
120	*	255.255.255.255	6	443	no	basic/safe-reset				0
130	*	255.255.255.255	6	*	no	basic/reset				0
140	*	255.255.255.255	17	5060	no	basic/sip				0
150	*	255.255.255.255	17	*	no	basic/default				0
160	*	255.255.255.255	1	*	no	permit	300	300	pps	0
170	*	255.255.255.255	*	*	no	basic/default				0
180	*	255.255.255.255	6	*	yes	basic/default				0
190	*	255.255.255.255	17	*	yes	basic/default				0
200	*	255.255.255.255	*	*	yes	basic/default				0

se@GUARD-conf-zone-Demo>



Quick Connect Profiles

```
se@GUARD-conf-zone-Demo>
se@GUARD-conf-zone-Demo>sh rates details
```

	pps	bps
Legitimate traffic:	0	0
Malicious traffic:	0	0

Details:

Received traffic:	0	0
Forwarded traffic:	0	0
Dropped traffic:	0	0
Replied traffic:	0	0
Spoofed traffic:	0	0

```
se@GUARD-conf-zone-Demo>show drop
```

	pps	bps	Packets	Kbits
Total Drop:	0	0	0	0
Dynamic filters:	0	0	0	0
User filters	0	0	0	0
Flex filter:	0	0	0	0
Rate limit:	0	0	0	0
Incoming TCP unauthenticated-basic:	0	0	0	0
Incoming TCP unauthenticated-strong:	0	0	0	0
Outgoing TCP unauthenticated:	0	0	0	0
UDP unauthenticated-basic:	0	0	0	0
UDP unauthenticated-strong:	0	0	0	0
Other protocols unauthenticated:	0	0	0	0
TCP fragments unauthenticated:	0	0	0	0
UDP fragments unauthenticated:	0	0	0	0
Other protocols fragments unauthenticated:	0	0	0	0
DNS malformed replies:	0	0	0	0
DNS spoofed replies:	0	0	0	0
DNS short queries:	0	0	0	0
Non DNS packets to/from DNS port:	0	0	0	0
Bad packets to proxy addresses:	0	0	0	0
TCP anti-spoofing features related pkts:	0	0	0	0
DNS anti-spoofing features related pkts:	0	0	0	0
Anti-spoofing internal errors:	0	0	0	0
SIP anti-spoofing features related pkts:	0	0	0	0
SIP malformed packets:	0	0	0	0
Land attack:	0	0	0	0
Malformed packets:	0	0	0	0

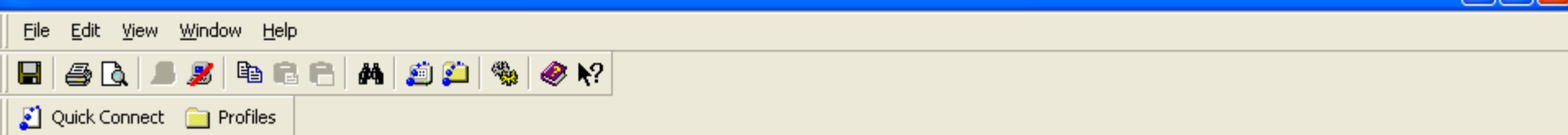
```
se@GUARD-conf-zone-Demo>
```

Show Counters Before the Attack

TFN Attack Tool

```
172.25.89.73 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles
1) Spoofed SYN (tfn)
2) Focused SYN (tfn)
3) Spoofed UDP (tfn)
4) Spoofed ICMP/PING (tfn)
5) Combined UDP/TCP/ICMP (tfn)
6) Spoofed TCP/SYNACK (tfn)
7) Spoofed TCP/FIN (tfn)
8) Spoofed IP/TCP fragments (tfn)
9) IP/UDP fragments (jolt2)
10) IP/ICMP fragments (trash)
11) IP/IGMP fragments (fawx)
12) Client attack
13) HTTP half connections
#? 1
Attack #1:
Protocol      : random
Source IP     : random
Client input  : single host
Sleep between packets :0 usecs
Command       : change spoof level to 7.0.0.008
Sending out packets: .
Running spoofed SYN (tfn) attack
Hit <Enter> to stop attack
Connected to 172.25.89.73  SSH2 - aes128-cbc - hmac-md5 - none 116x19
```

Launch the Spoofed TCP SYN Attack.



```
Policy: tcp_services/any/analysis/syns/dst_port

se@GUARD-conf-zone-Demo>se@GUARD-conf-zone-Demo>show dynamic-filters details
ID   Action                               Exp Time Source IP      Source Mask      Proto DPort Frg RxRate(pps)
7    to-user-filters                       353          *                255.255.255.255 6      *    no N/A
    Attack flow: 6 *
    Triggering rate: 250000.00 Threshold: 50.00
    Policy: tcp_services/any/analysis/syns/dst_port
8    to-user-filters                       353          *                255.255.255.255 6      80   no N/A
    Attack flow: 6 *
    Triggering rate: 272727.28 Threshold: 150.00
    Policy: tcp_services/any/analysis/syns/dst_port
```

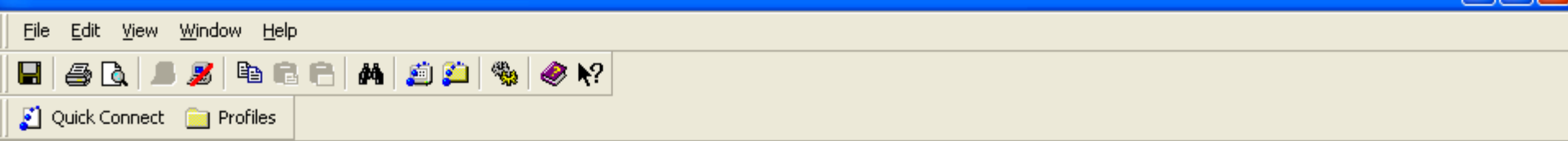
```
se@GUARD-conf-zone-Demo>show drop

Total Drop:                pps      bps      Packets      Kbits
Dynamic filters:           0         0         0             0
User filters                0         0         0             0
Flex filter:                0         0         0             0
Rate limit:                 0         0         0             0
Incoming TCP unauthenticated-basic: 0         0         0             0
Incoming TCP unauthenticated-strong: 0         0         0             0
Outgoing TCP unauthenticated:    0         0         0             0
UDP unauthenticated-basic:       0         0         0             0
UDP unauthenticated-strong:     0         0         0             0
Other protocols unauthenticated: 0         0         0             0
TCP fragments unauthenticated:  0         0         0             0
UDP fragments unauthenticated:  0         0         0             0
Other protocols fragments unauthenticated: 0         0         0             0
DNS malformed replies:         0         0         0             0
DNS spoofed replies:          0         0         0             0
DNS short queries:             0         0         0             0
Non DNS packets to/from DNS port: 0         0         0             0
Bad packets to proxy addresses: 0         0         0             0
TCP anti-spoofing features related pkts: 0         0         0             0
DNS anti-spoofing features related pkts: 0         0         0             0
Anti-spoofing internal errors:  0         0         0             0
SIP anti-spoofing features related pkts: 0         0         0             0
SIP malformed packets:         0         0         0             0
```

Two Dynamic Filters Are Added:
The two flows under “Analysis” mode are triggered with this attack.

Action is “to-user” filters keying off protocol (6); destination port (80).

Because it is higher than the thresholds (50 and 150 as seen), the action is to forward it off to the user filters.



```
Zone is in PROTECT mode
Operation Mode: AUTOMATIC
Policy thresholds are TUNED
Activation start time: Nov 15 10:32:15
Description:
Zone ID: 1019 (Guard/Detector)
Template: GUARD_DEFAULT
Activation-Interface: zone-name-only
Activation-Extent: ip-address-only
Protection-End Timer: forever
Filter-termination filter-rate      threshold: 2.00 pps
Filter-termination zone-malicious-rate threshold: 50.00 pps
Attack-detection zone-malicious-rate threshold: 10.00 pps
RATE: no-limit

SUBNET: 192.168.3.0 255.255.255.0
                pps          bps
Legitimate traffic: 0          305
Malicious traffic: 76992      39420123
```

Because there is no legitimate traffic, all the malicious spoofed traffic is caught by the user filters.

Almost *all* the traffic is caught by user filter.

```
There are 2 dynamic filters
There are no bypass filters
```

**** USER FILTERS ****

Row	Source IP	Source Mask	Proto	DPort	Frg	Action	Rate	Burst	Units	RxRate(pps)
10	*	255.255.255.255	6	80	no	basic/redirect				77084
20	*	255.255.255.255	6	8080	no	basic/redirect				0
30	*	255.255.255.255	6	8000	no	basic/redirect				0
40	*	255.255.255.255	6	8008	no	basic/redirect				0
50	*	255.255.255.255	6	8081	no	basic/redirect				0
60	*	255.255.255.255	6	3128	no	basic/redirect				0
70	*	255.255.255.255	6	53	no	basic/dns-proxy				0
80	*	255.255.255.255	6	25	no	basic/safe-reset				0
90	*	255.255.255.255	6	110	no	basic/safe-reset				0
100	*	255.255.255.255	6	143	no	basic/safe-reset				0
110	*	255.255.255.255	6	6667	no	basic/safe-reset				0
120	*	255.255.255.255	6	443	no	basic/safe-reset				0
130	*	255.255.255.255	6	*	no	basic/reset				0
140	*	255.255.255.255	17	5060	no	basic/sip				0

--More--

GUARD

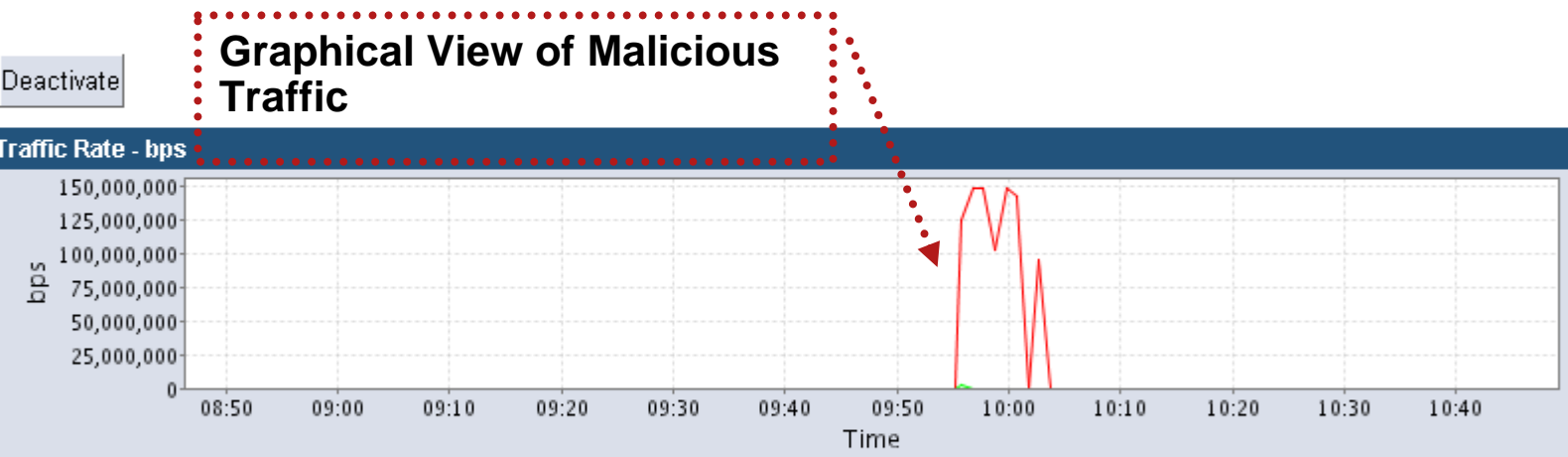
November 20, 2006 10:46

User name: s
Privileges: dynam

- Main
- Diagnostics
- Protection
- Learning
- Configuration

Zone Demo (automatic) - Protected

- Guard
- Guard Summary
- Protected Zones (1)
 - Demo
- All Zones (4)
 - Demo
 - terry
 - tme
 - Worm



Legitimate rate:	Min.: 0.0	Max.: 2,215,458.0	Avg.: 17,910.27	Cur.: 0.0
Malicious rate:	Min.: 0.0	Max.: 149,340,466.0	Avg.: 7,376,020.73	Cur.: 0.0

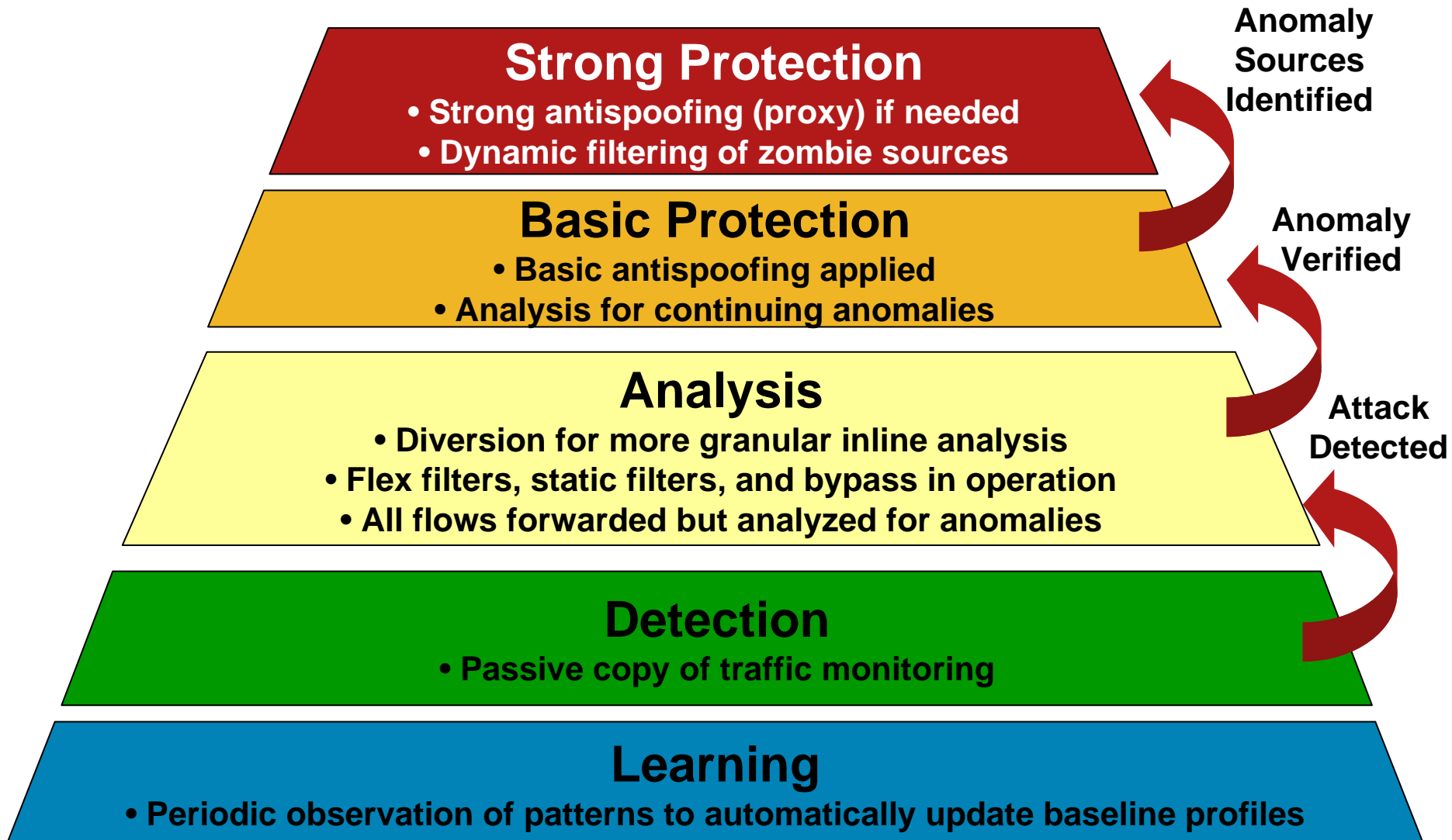
Zone status

Active Dynamic filters:	0	Last attack time:	Nov 20, 09:55:20
Pending Dynamic filters:	0	Activation time:	Nov 15, 10:32:15

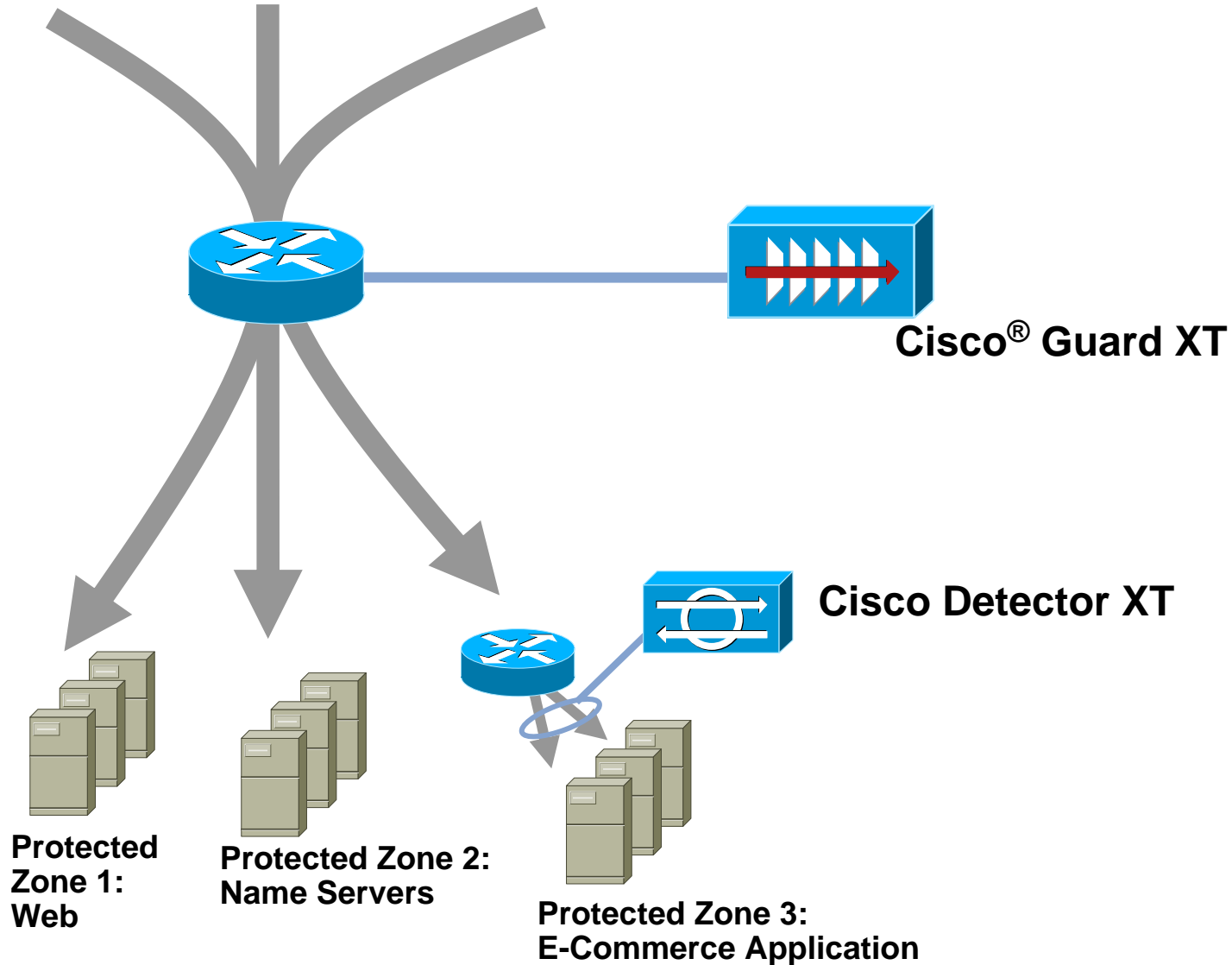
Recent Events

Time	Severity	Type	Details
Nov 20 10:15:20 2006	Malic	attack ended	Attack ended

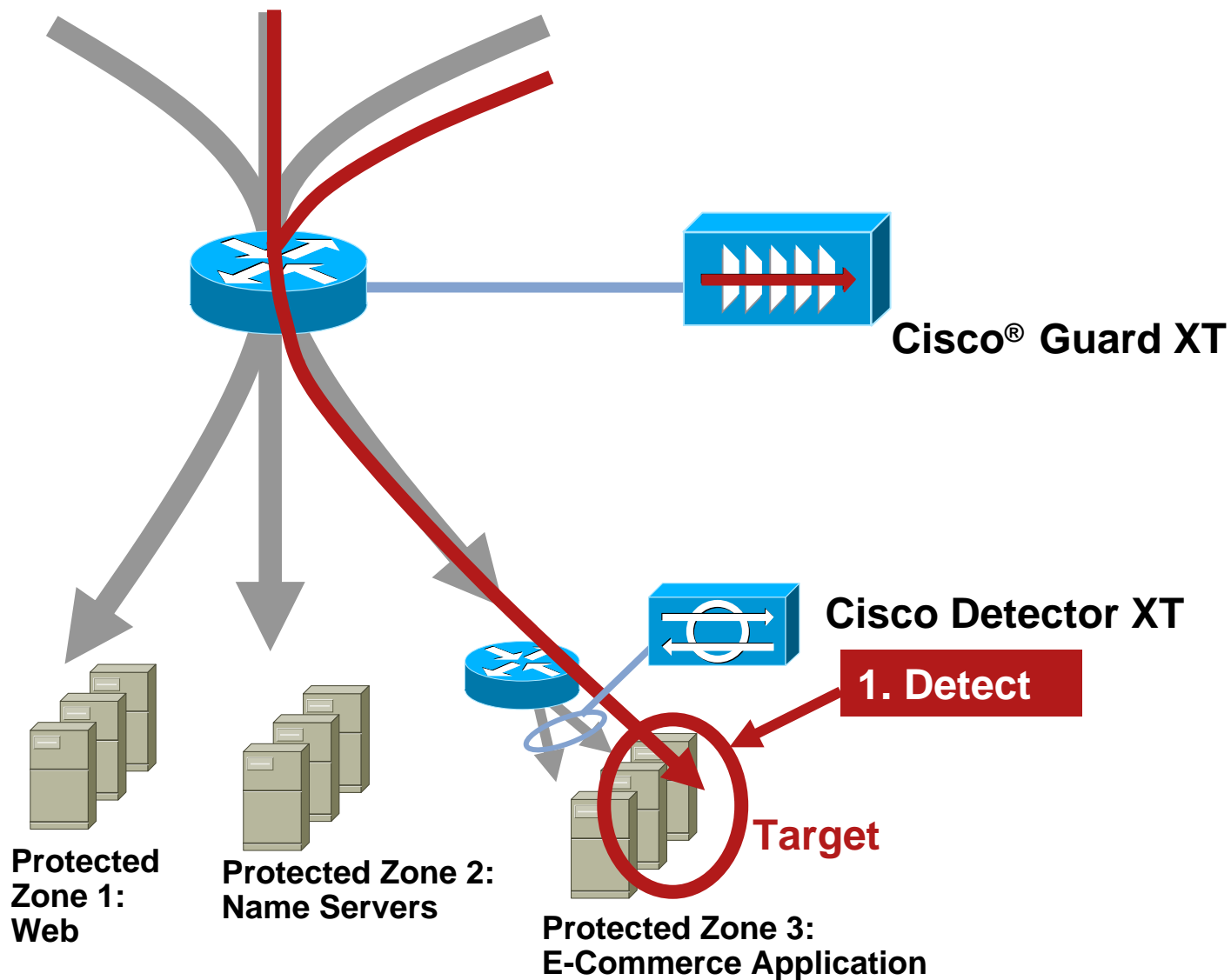
Packet Flow Through the Defense Modules



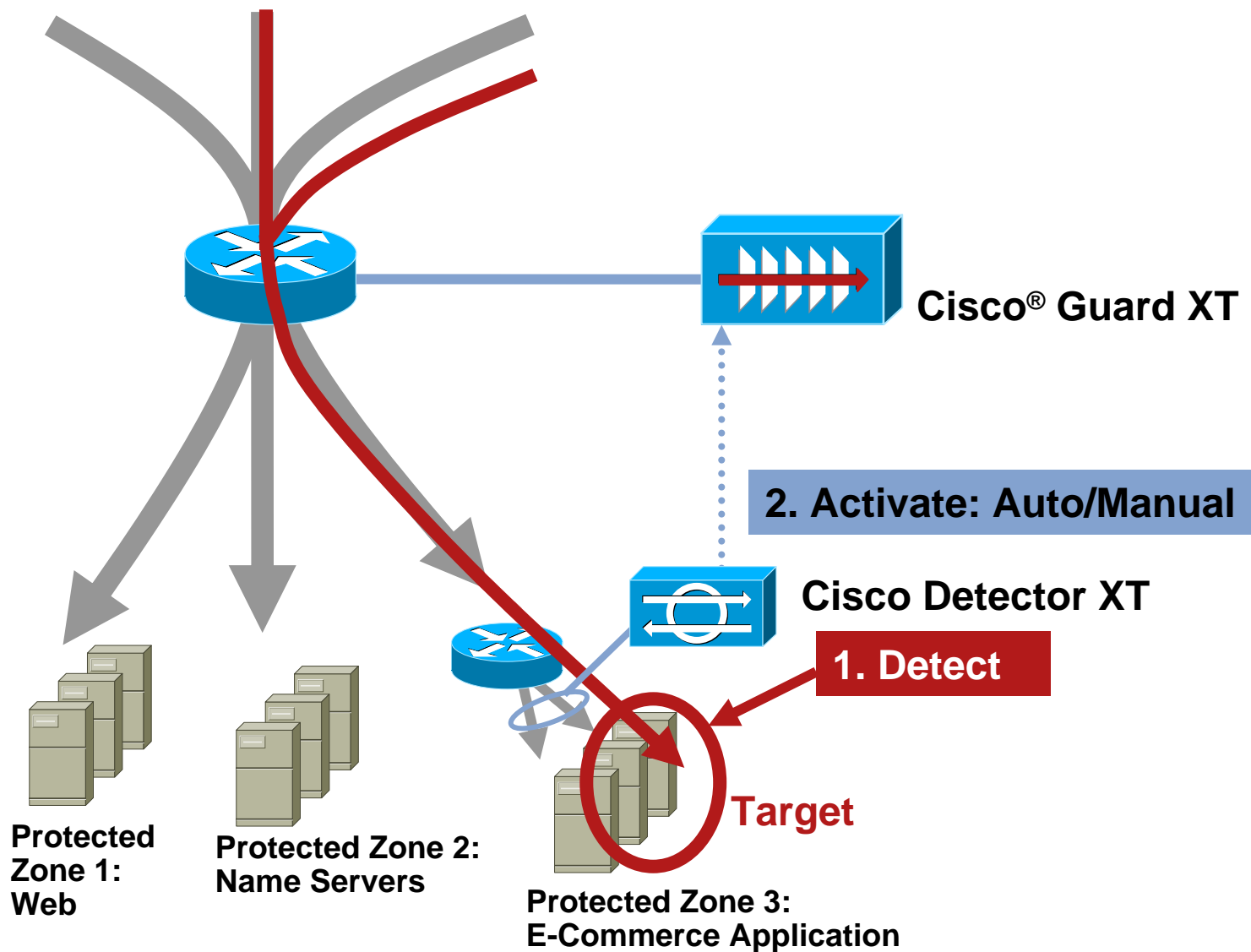
Cisco DDoS Solution



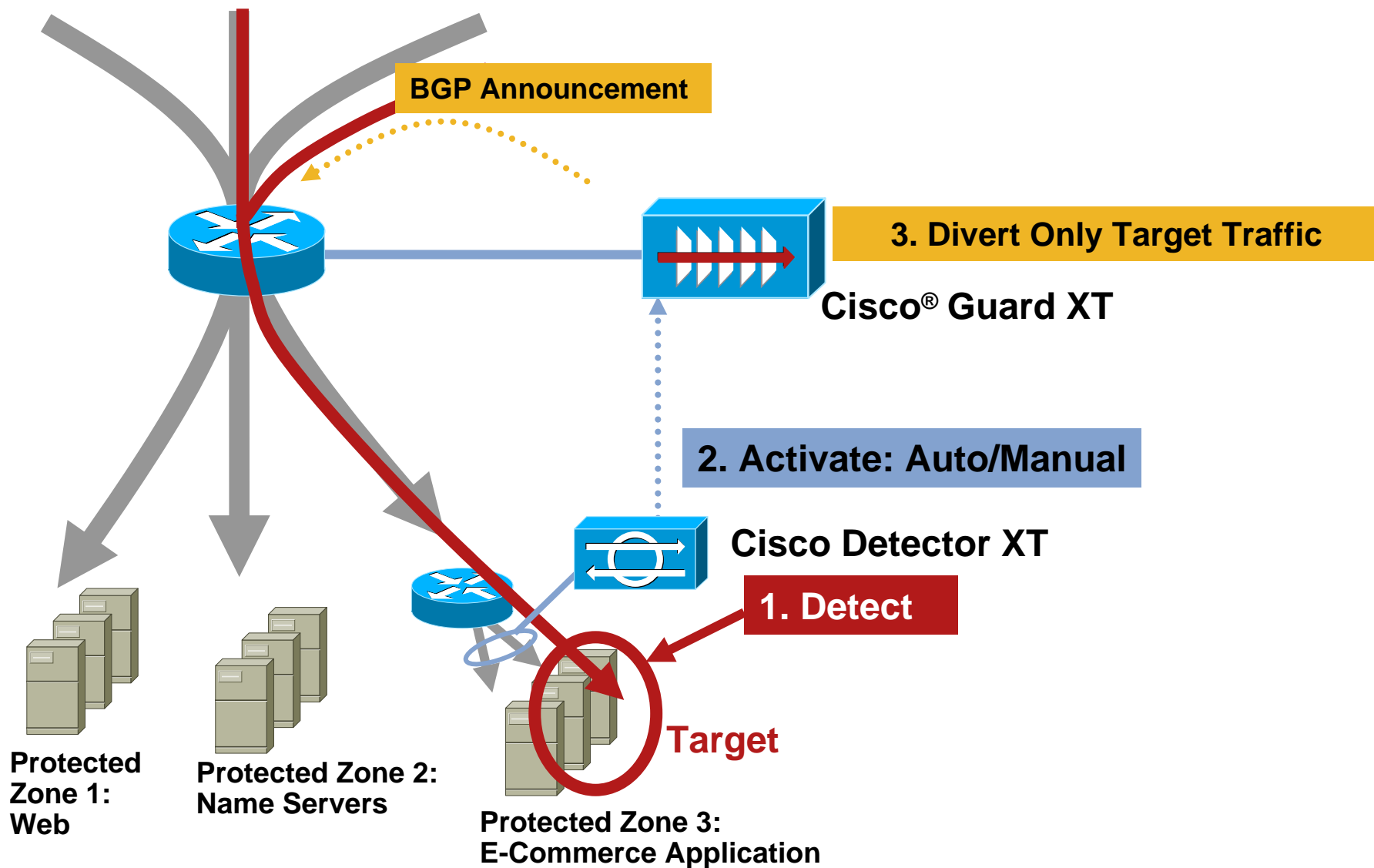
Cisco DDoS Solution



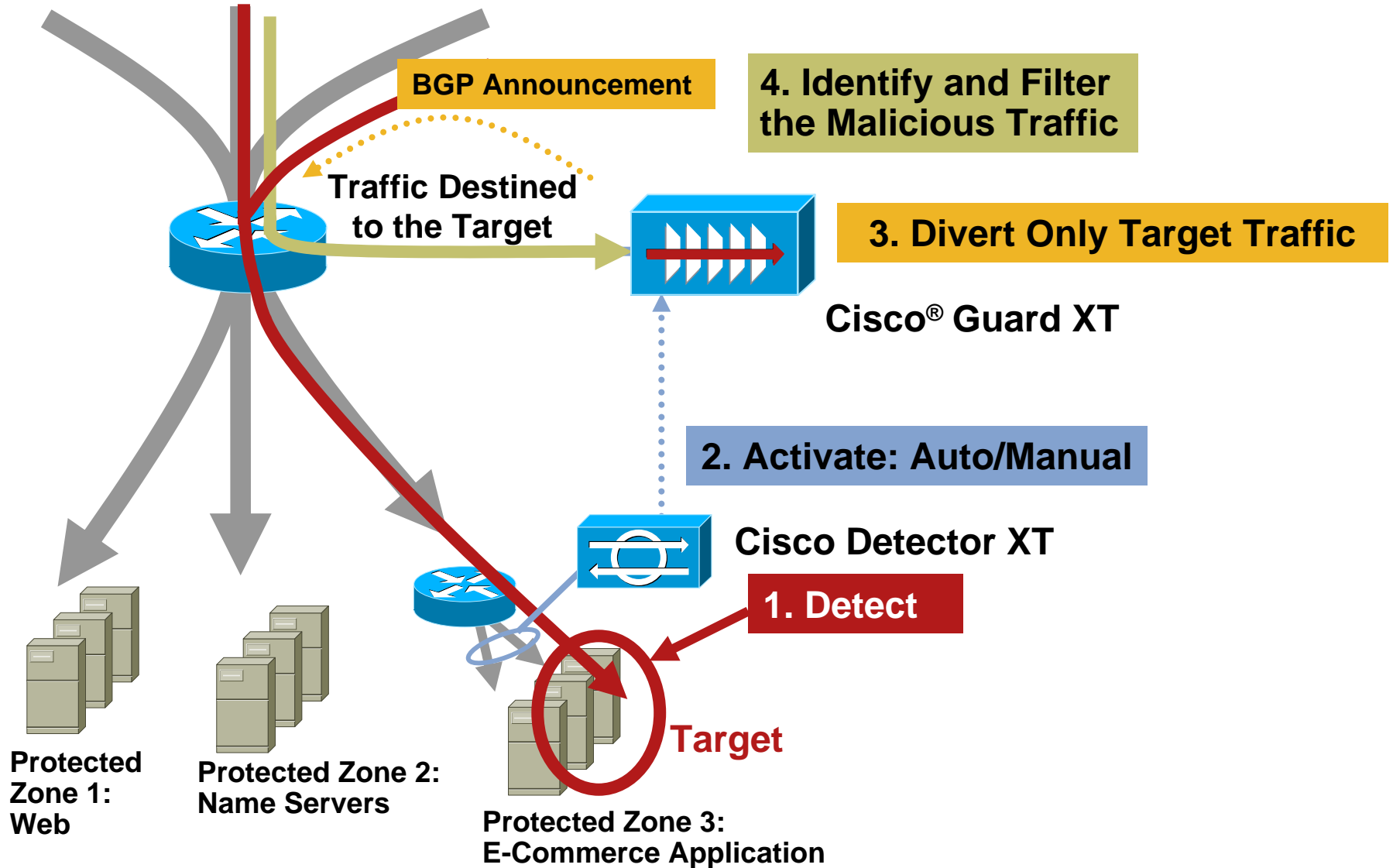
Cisco DDoS Solution



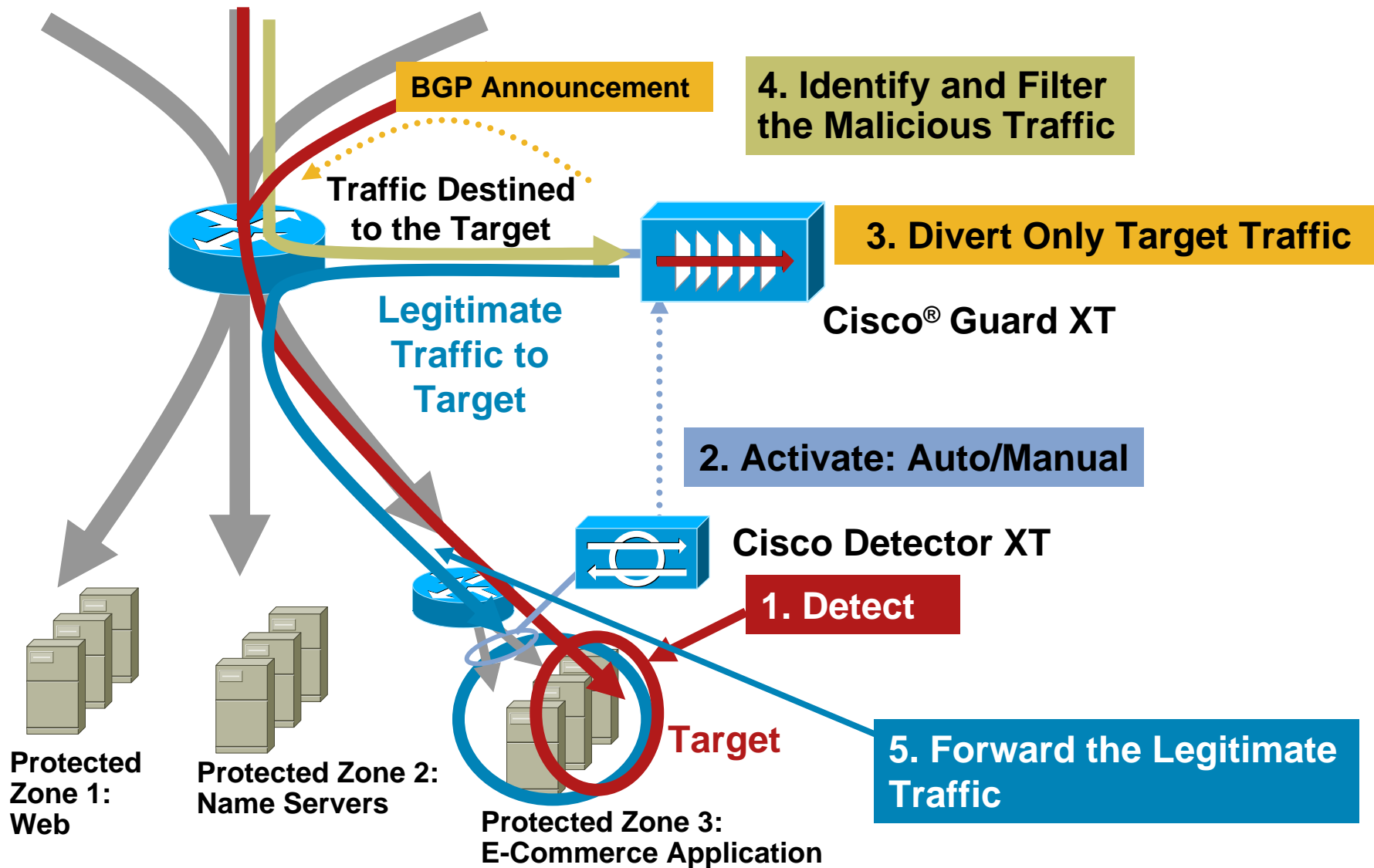
Cisco DDoS Solution



Cisco DDoS Solution



Cisco DDoS Solution



Cisco DDoS Solution

