Security Toolsets for ISP Defense

Backbone Practices

Authored by Timothy A Battles (AT&T IP Network Security)

What's our goal?

To provide protection against anomalous traffic for our network and it's customers.

What is anomalous traffic?

Infiltration of viruses.

Spreading of Worms.

Denial of Service Attacks.

Effects of route theft.

Port scanning.

Network enumeration.

Effects of an exploited vulnerability.

What defines protection?

There are 5 different components that must be acted upon in order to reduce the effects of anomalous traffic.

Component 1: Prevention

Component 2: Prediction

Component 3: Detection

Component 4: Mitigation

Component 5: Prosecution

What is prevention?

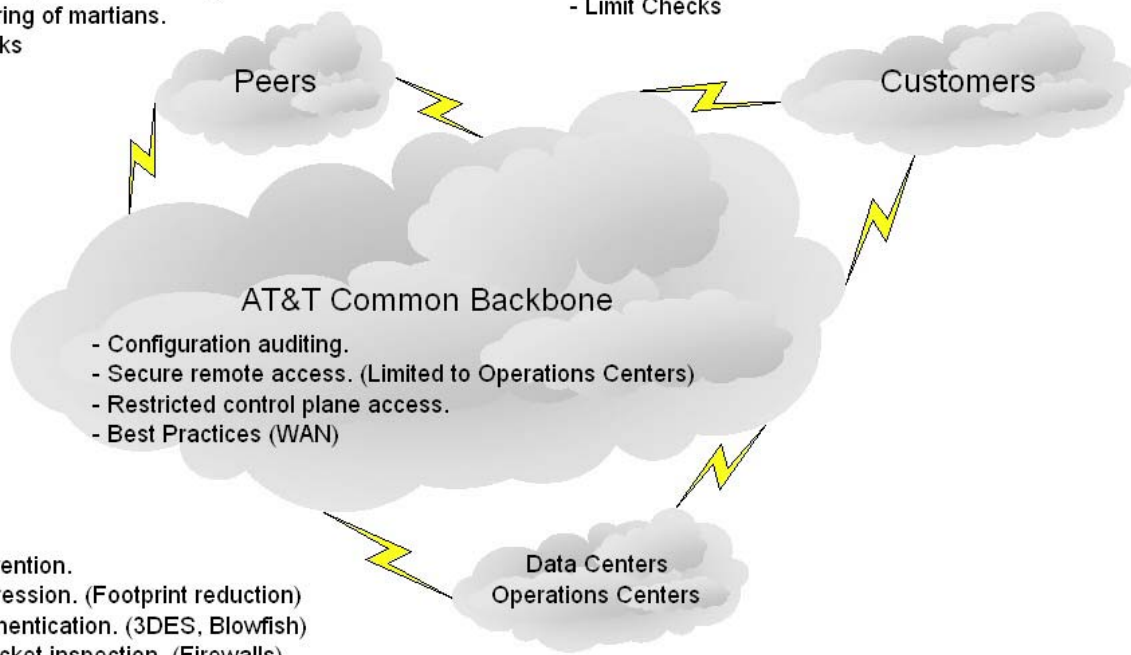
Prevention entails the ability to prevent someone from launching an anomalous attack from/or against your network. Prevention on the backbone includes some of the following items.

1. Spoof Prevention at the edge.
2. Control plane protection.
3. Route suppression and dampening.
4. Routing protocol protection.

How is this implemented?

- Spoof prevention of management blocks.
- Infrastructure protection for backbone devices.
- Authentication and encryption for routing protocols.
- Reverse path checking.
- Route dampening.
- Control plane protection for edge devices.
- Route filtering of martians.
- Limit Checks

- Spoof prevention of management blocks.
- Infrastructure protection for backbone devices.
- Spoof prevention.
- Route dampening.
- Control plane protection for edge devices.
- Specific route filtering.
- Limit Checks



- Spoof prevention.
- Route supression. (Footprint reduction)
- Strong authentication. (3DES, Blowfish)
- Stateful packet inspection. (Firewalls)
- Deep packet inspection. (IDS Sensors)
- Secure remote access.
- Separation of services.
- Best Practices (LAN)

Prevention Toolsets

- Configuration Auditing
  - Global access-list audits.
  - Route-map audits.
  - VTY, CON, and AUX audits.
  - Service audits.
  - AAA audits.

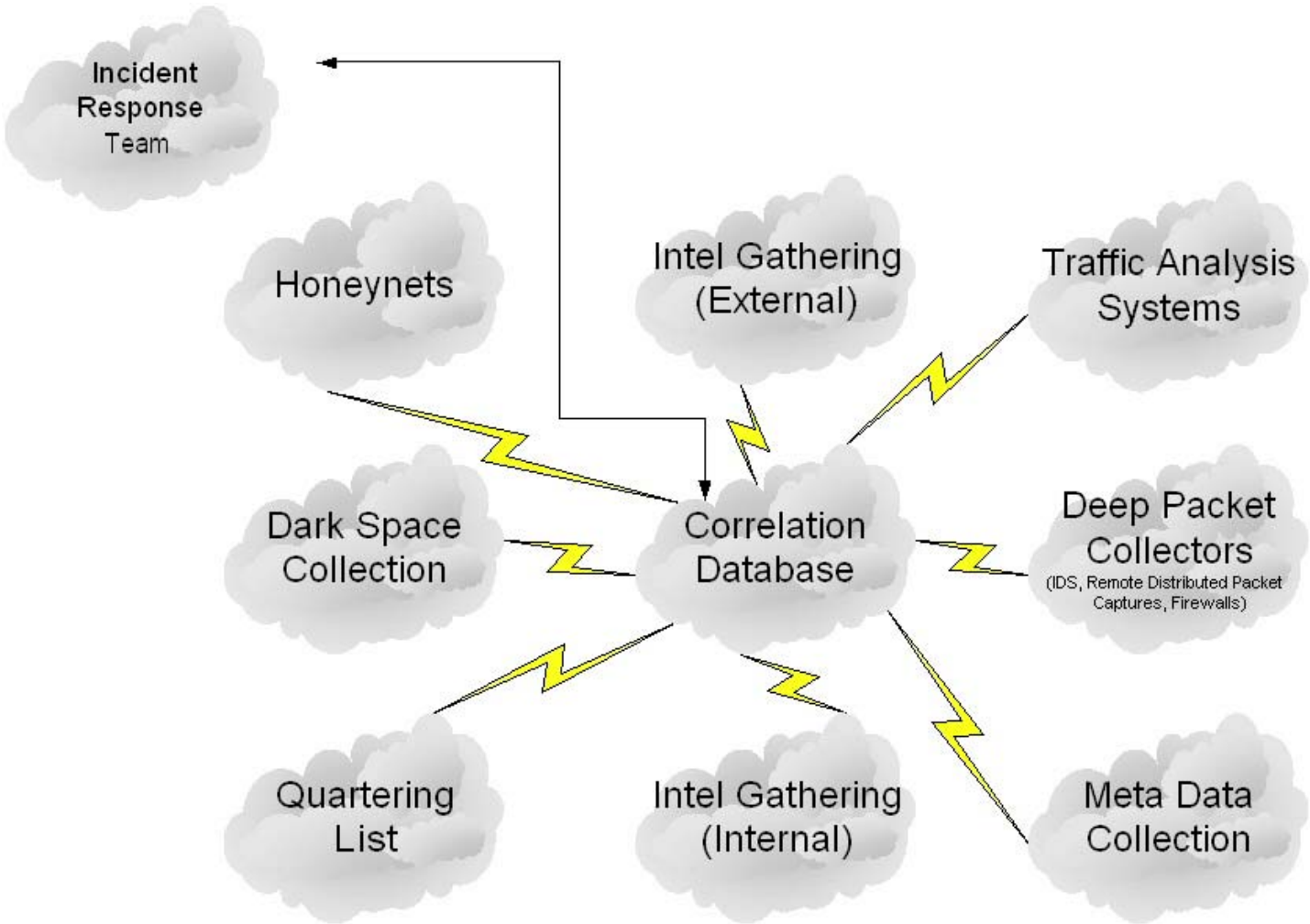
    Router configurations are downloaded 4 times daily to a data warehouse. Queries are performed against approved templates to perform exception reports.

What is prediction?

Prediction is a proactive approach to dealing with anomalous traffic. Prediction does not necessarily forecast when an attack will occur, but can often forecast type, strength, and sometimes the where. The following items should be performed in an effort to predict areas of threat.

1. Analysis of port scanning and enumeration. (Breach)
2. Detection of Distributed Agents. (DOS)
3. Dark Space analysis. (Worms)

How is prediction implemented?



Prediction Toolsets

- Data Mining (Correlation Database)
  - Customer X is a financial institution who has just been involved in a blackmail DOS attack. Customer Y another financial institution is attacked 4 days later. With the frequency of DOS attacks correlation is becoming more tedious for human correlation simple DB Mining can be used to make the correlation and potentially alert similar customer types. Correlations can be made on day of week or month most likely, source AS's, type of attack, strength of attack, and duration of attack.

Prediction Toolsets (Cont.)

- Quartering List
  - A C&C is discovered. The addresses is blackholed or sinkholed, but no analysis is being performed. Quartering list typically are automatically generated for abuse to have records of what customers are infected for cleanup, but Quartering list can also provide prediction. Rapid declines in quartering list can determine that a new controller has been added. New DOS attacks can be analyzed to forefront repetitive infected clients. Flow data for these repetitive infected clients can be monitored for discovery of new command and control platforms.

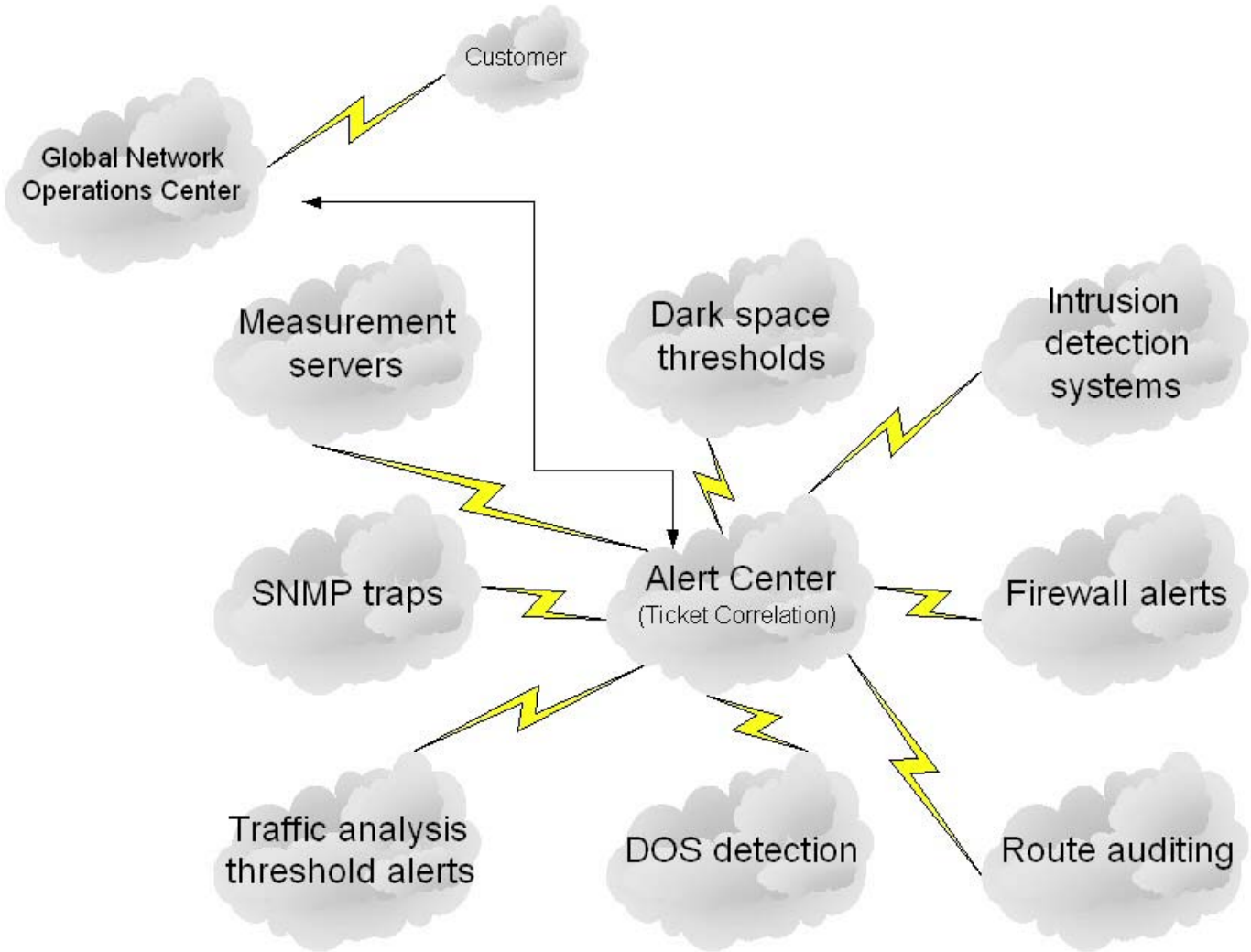
Prediction Toolsets (Cont.)

- Dark Space and Honeynets
  - Dark space and Honeynet can be used to predict trends in worm activity. Dark space collectors that are flow based can utilize source IP and protocol pairs over X amount of time to baseline activity.
  - Honeynets can be used to provide ack responses in order to validate known signatures and alert to new ones.

What is Detection?

Detection is the ability to make aware the appropriate parties that anomalous traffic is transiting the network.

How is detection be implemented?



Detection Toolsets

- Measurement Servers
  - Servers that send out ICMP, UDP, and TCP request to other measurements servers around the networks reporting back latency and packet loss. Can isolate problems within a general region.
- SNMP Traps
  - Can isolate and correlate over utilization of CPU or Memory on individual nodes.
- Traffic Analysis
  - Can isolate and correlate that CPU and memory increases are due to a over utilization of backbone links.

Detection Toolsets (Cont.)

- Dark Space Thresholds, DOS Detection, and Route Audits.
  - Can isolate and correlate that over consumption of resources is the direct result of a route change, a worm, or a DOS attack.
  - Additional heuristics can be performed. For denial of service attacks historical BGP records can be utilized to immediately determine the relevancy and determine the customer.

Detection Toolsets (Cont.)

- Dark Space Thresholds, DOS Detection, and Route Audits.
  - Route audits can determine whether or not this was an impact due to operations or perhaps route theft from an outside entity. Accounting logs can be data mined to determine what entries were made. Historical route views can be mined to determine what blocks and what external carrier was is responsible.

Process Example

All remote locals report latency to **ABCLOCAL**

SNMP Trap is sent from **HUB ROUTERA** of **ABCLOCAL**

Traffic Analysis reports that **HUB ROUTERA**'s uplinks are overutilized.

Upstream DOS detection systems reports a UDP Fragment Flood destined to **A.B.C.D/32**

Route Database reports that the Originator **of A.B.C.D/32** is **ACCESS ROUTER A of ABCLOCAL**

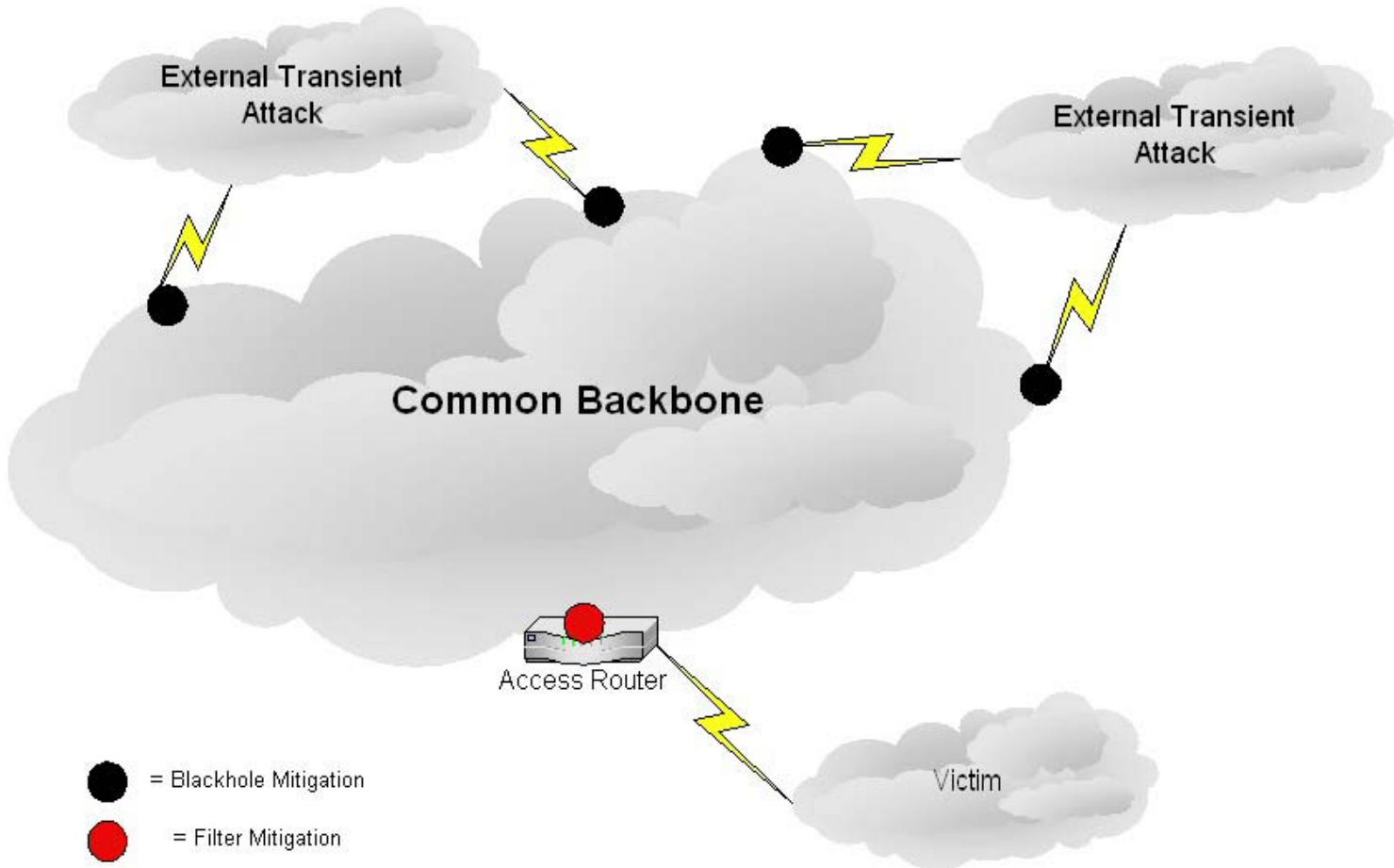
Trouble ticket is populated with information from all alerts. Operations proceeds to blackhole **A.B.C.D/32**

What is mitigation?

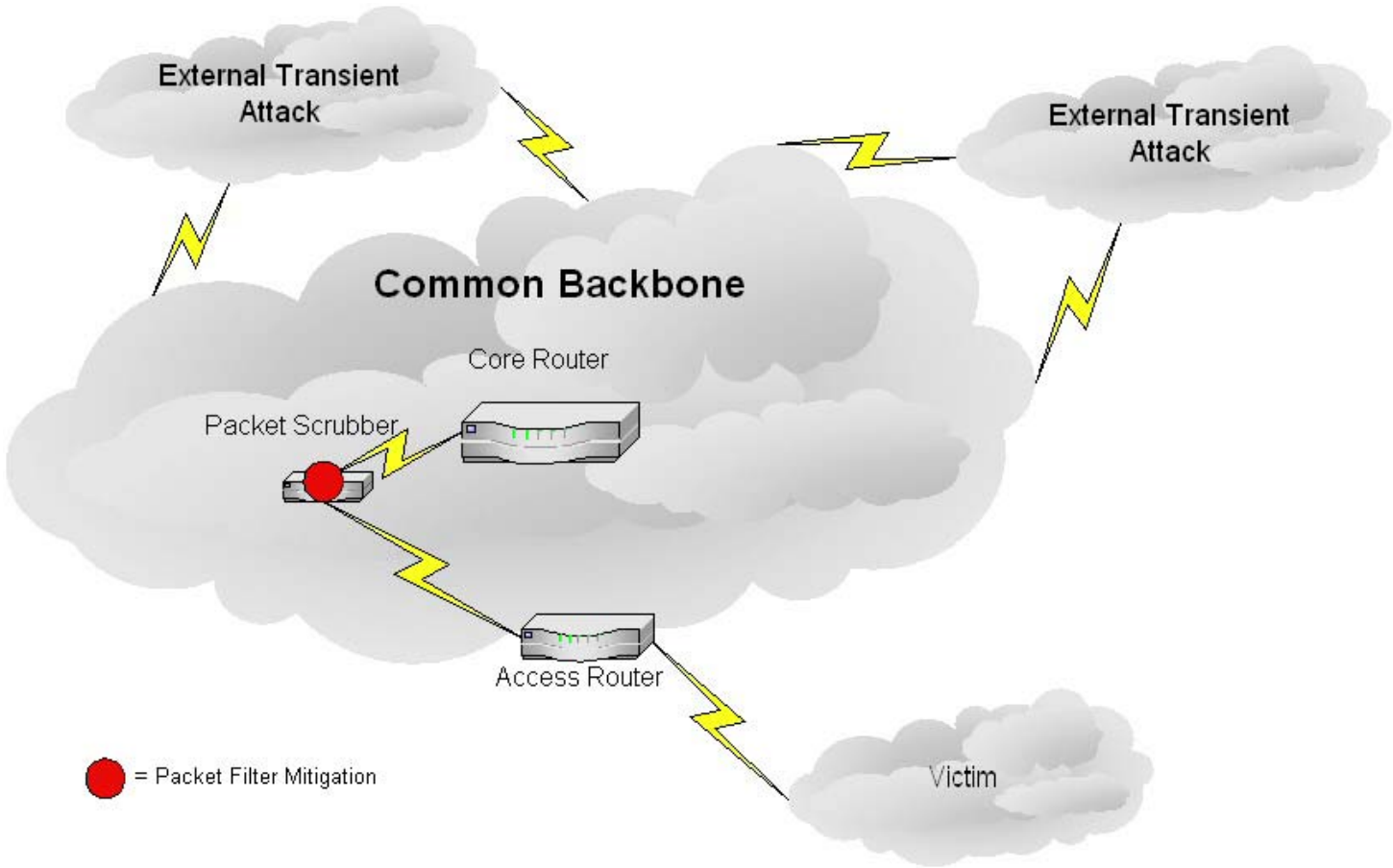
Mitigation is the end-all. Without it, no amount of prediction or detection will benefit the victim of a denial of service attack. Mitigation is the ability to stop an attack, or at the very least minimalize it once it has been detected. The following methods are generally accepted in terms of mitigation.

1. Blackholing
2. Packet Filtering
3. Packet Diversion

Perimeter Remote Triggered Blackholes and Packet Filtering



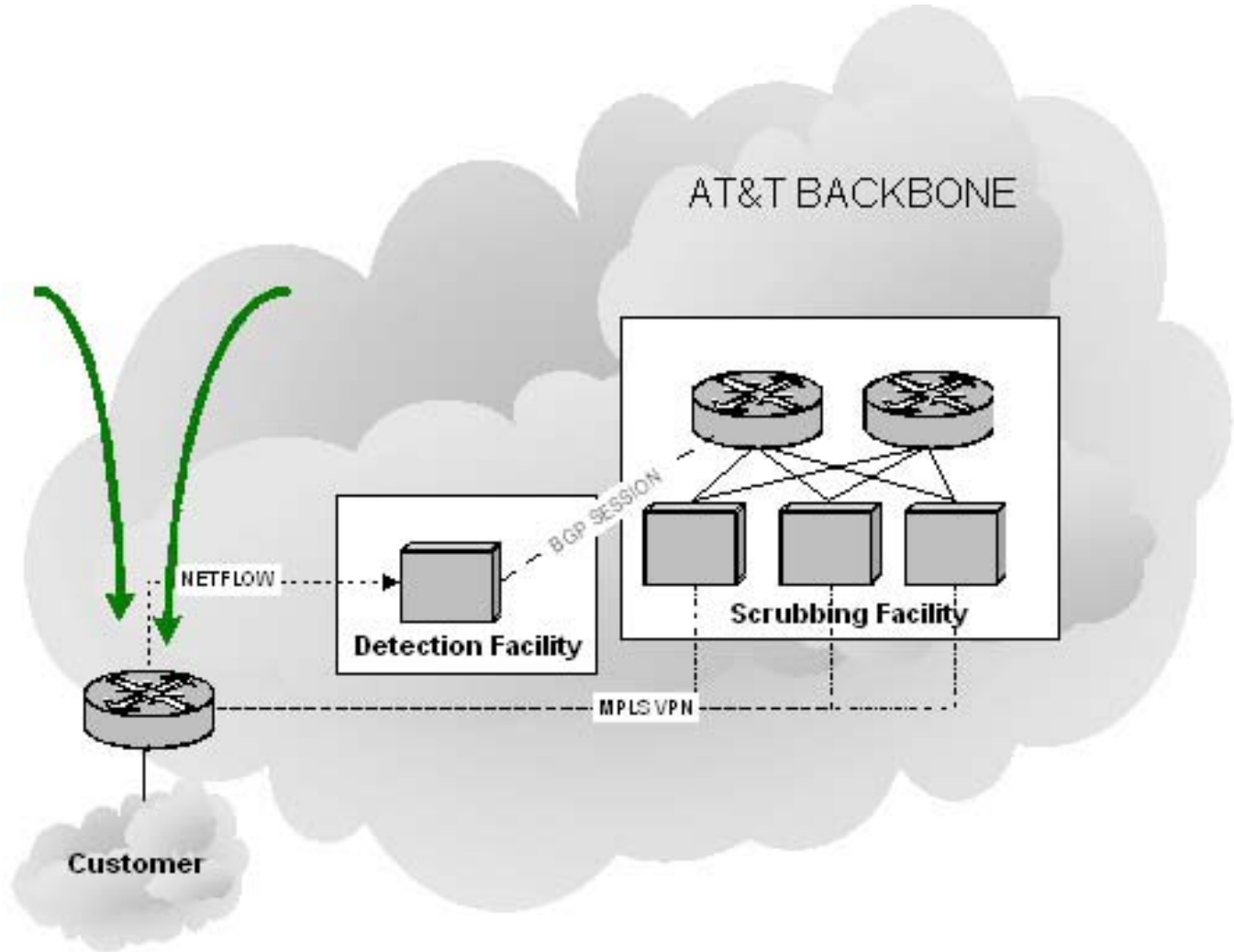
Packet Scrubbing



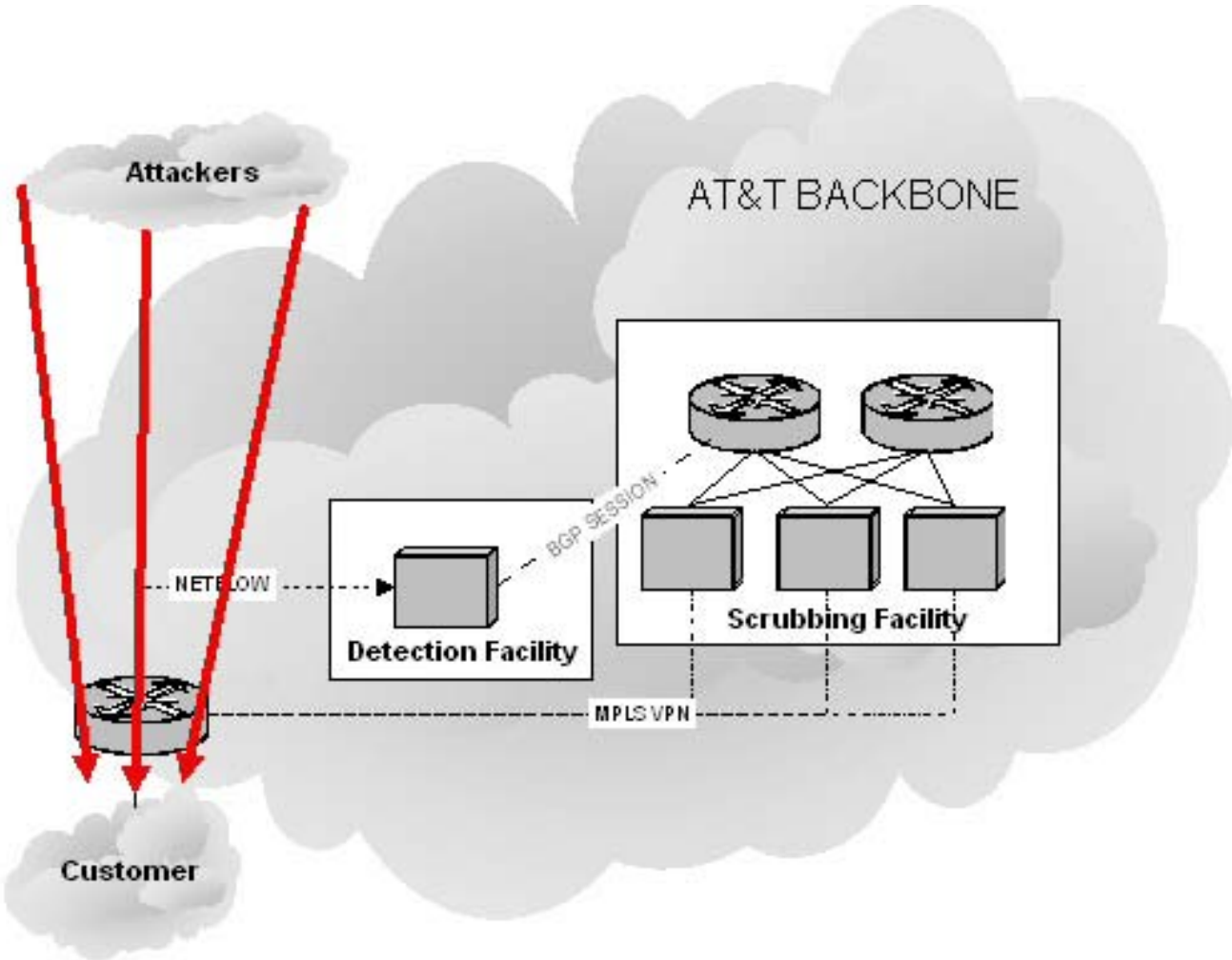
Toolsets for Mitigation

- Dedicated and Centralized Blackhole routers
  - Provides a centralized repository for malicious routes.
  - Provides stability because its not part of the backbone.
  - Can be utilized for sinkholing. Forensics facilities can be homed off it.
  - BGP sessions can be established to other internal systems that require blackhole mitigation.

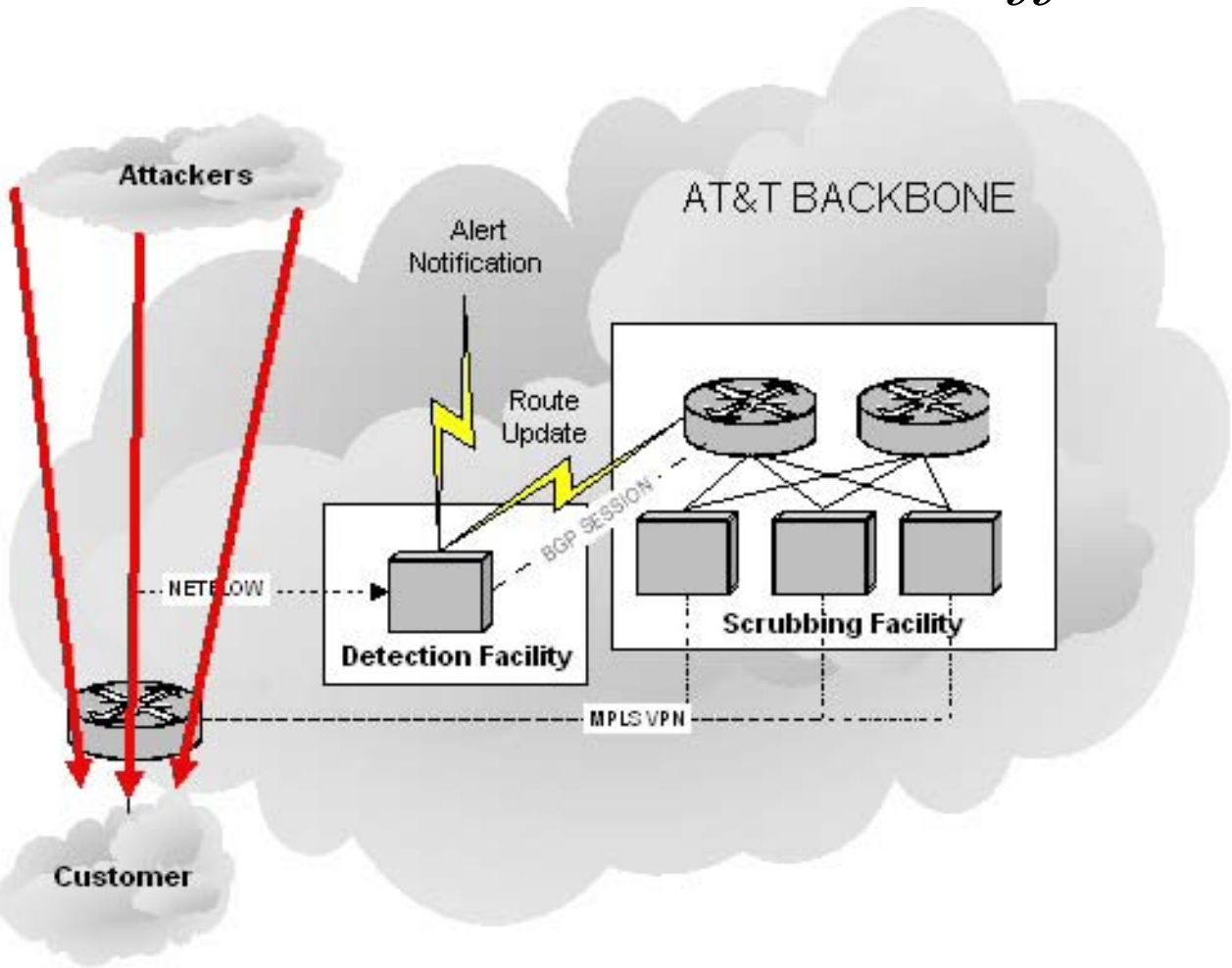
Traffic flows normally when no traffic anomalies are present.



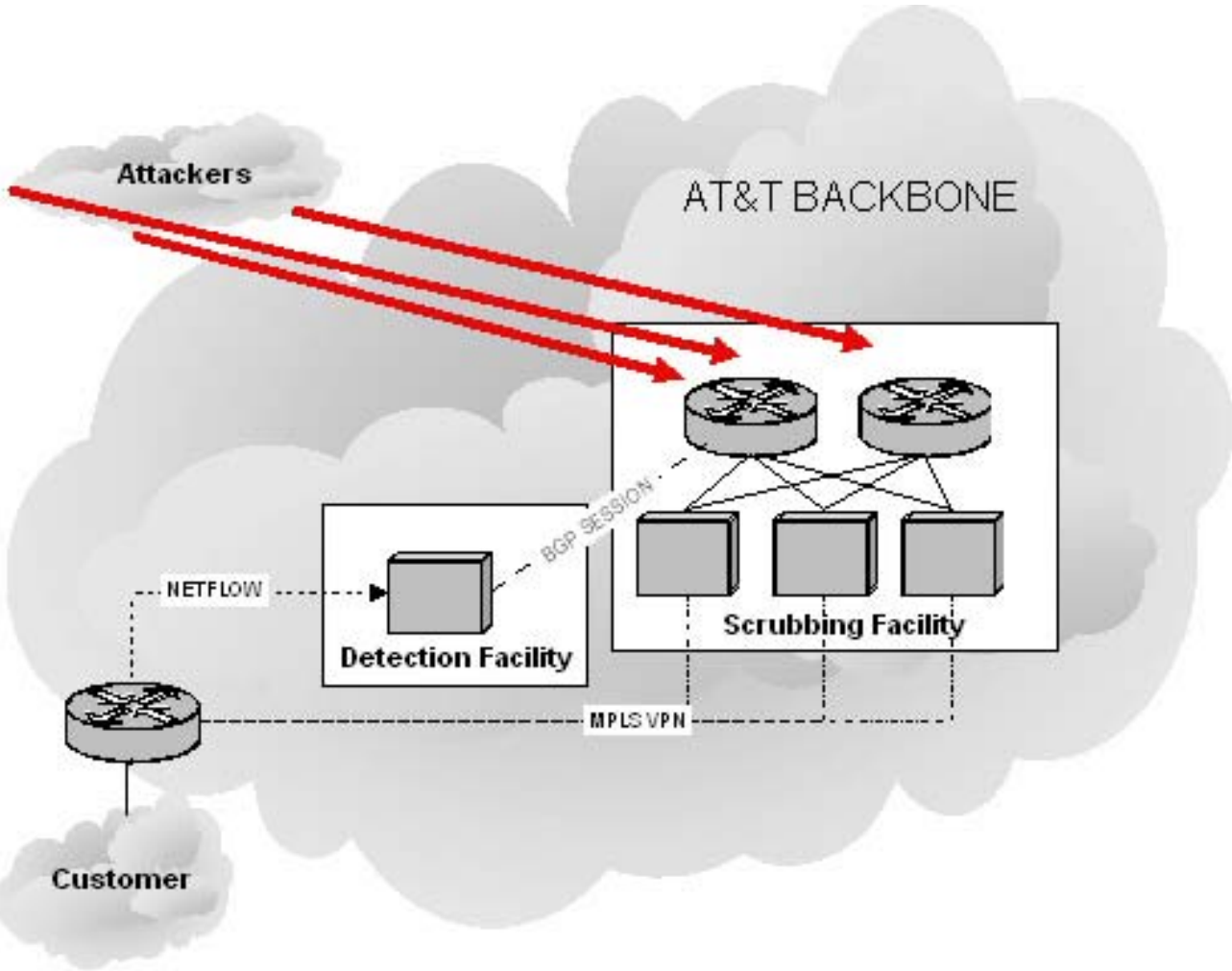
Attack Starts



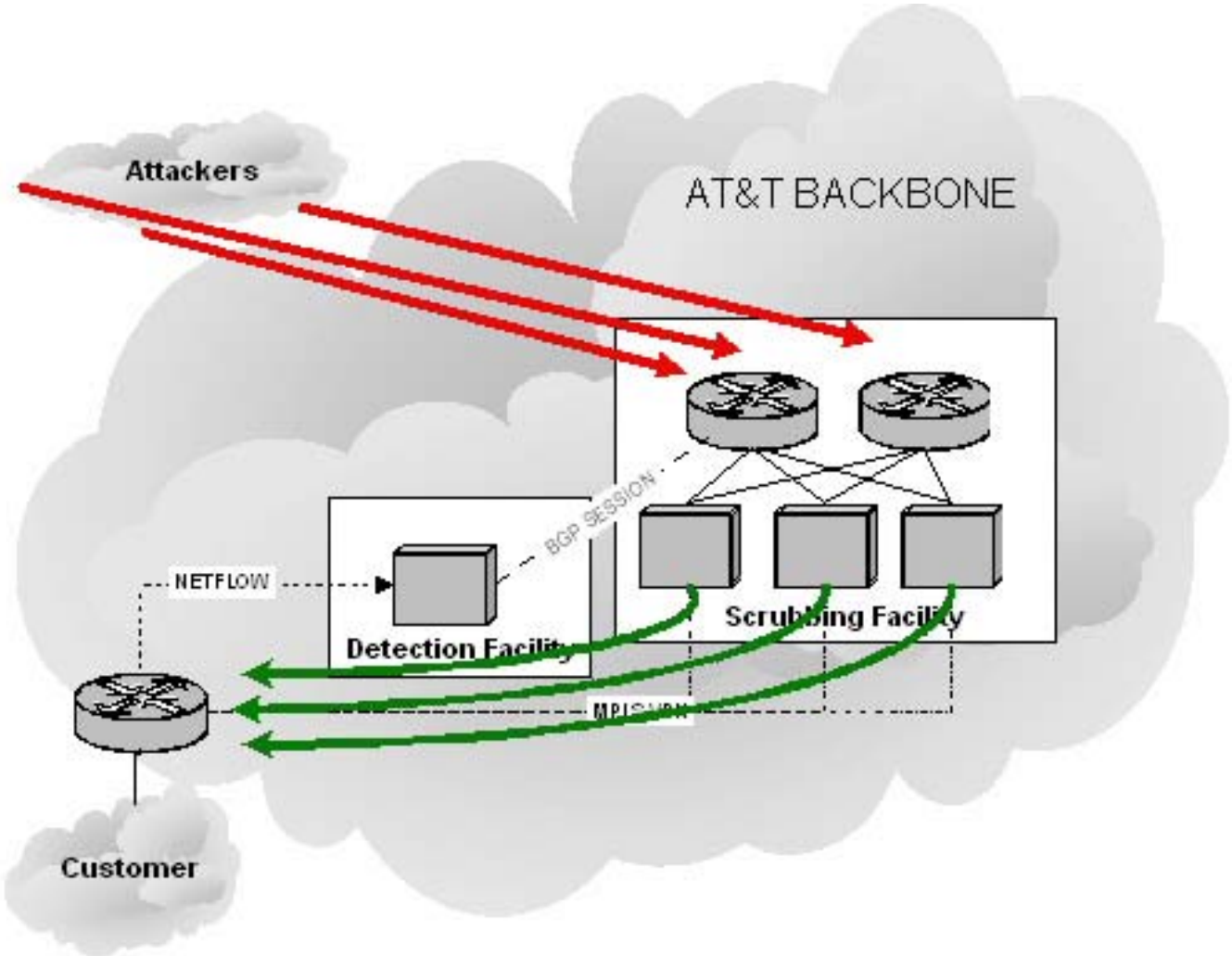
Attack is detected by network based netflow detectors. Alerts and route update is sent out to divert traffic.



Traffic is diverted to the scrubbing facility. Mitigation thresholds distinguish between valid and non-valid sources.



After malicious traffic is scrubbed, valid traffic is delivered back to the customer

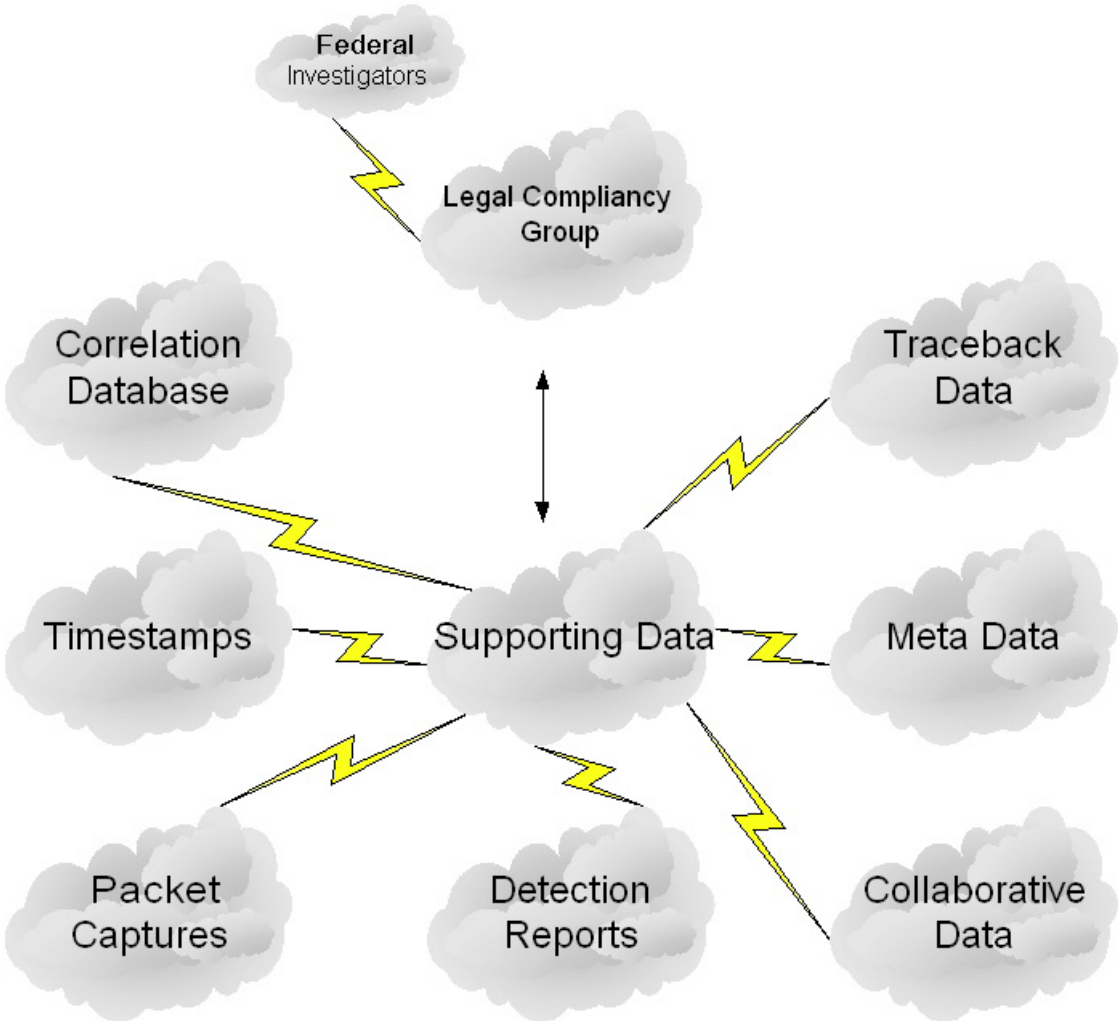


Prosecution

The ability to identify and aide in the prosecution of the attacker.

- Legal Compliancy
- Rapid Response
- Internal/External Communication Links

What is supporting data?



Thankyou

Timothy A Battles

AT&T IP Security