

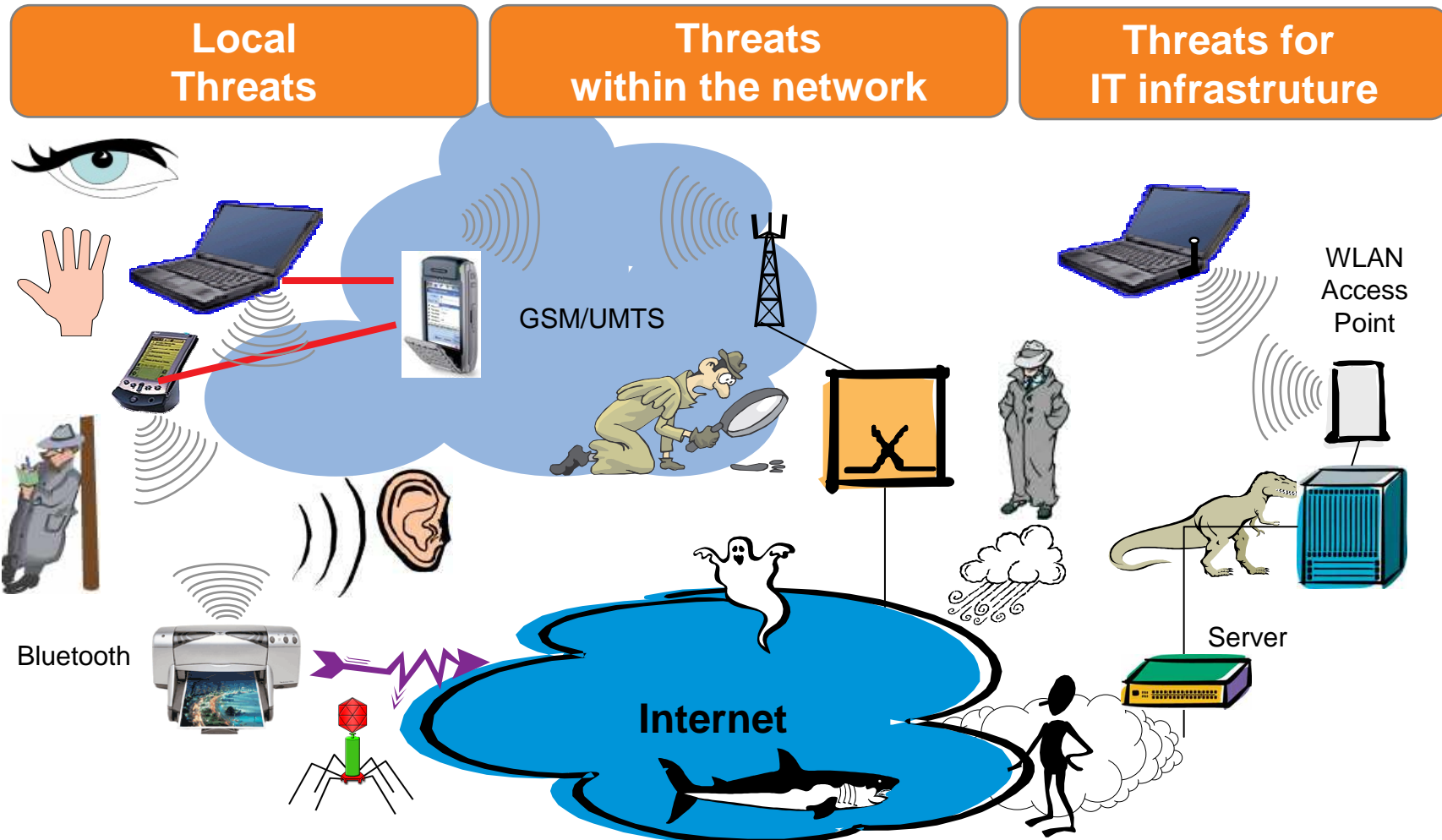


Securing Large Scale VoIP Infrastructures

Alexander Hoffmann, CEO

- PSTN is 100% secure
 - True, as long as no one manages to get to the cables at the street corner
- Firewalls solve all security issues
 - Cutting off your Internet cable would solve them as well
- NAT is a great security feature
 - Sure, if you like complex things

General Threats



- SPIT, SPIM, VoIP DoS: Hype or Reality
 - Today Hype tomorrow Reality
- Reality
 - No Script kiddies yet
 - Immature user agents
 - Mis-configured proxies and gateways
 - Inaccurate CDRs
 - Too stringent firewalls and mis-configured NATs
- DNS traffic up-to 90% mainly junk

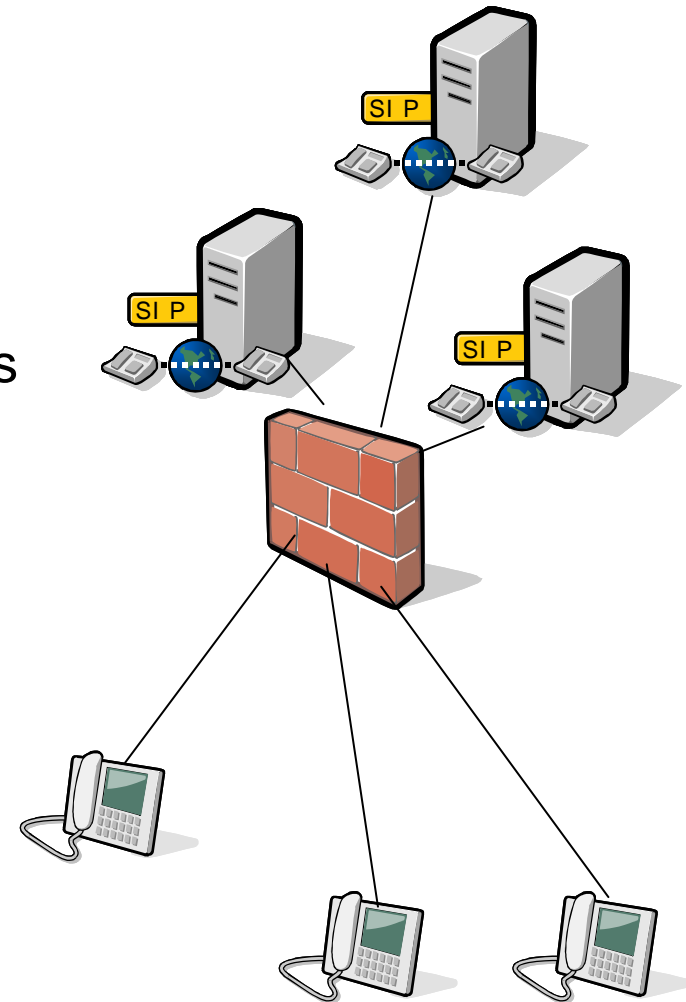
- More subscribers means more revenue but:
 - More signaling traffic to deal with
 - More heterogeneous devices
 - More database entries
 - Higher possibilities of denial of service
 - Higher costs of failure
- Security solutions
 - Must be standards conform
 - Must scale to millions of users
 - Must support all NAT scenarios
 - Must not expect any changes or cooperation from the user agents
 - Must be highly reliable in terms of signaling processing and data

- Possible issues
 - Flooding attacks
 - Misconfigured users
 - Malicious users
 - SPAM
- Memory: SIP is memory hungry
 - Save messages while processing them
 - Save messages during transactions up to a few minutes
- CPU:
 - Message parsing
 - Application execution
- Bandwidth
 - Nothing special here
- Related issues
 - DNS
 - TCP/TLS to non responding servers

- Brute force: Start thousands of calls with different FROM, TO and call-ID
- Broken Sessions:
 - Start sessions and do not complete
 - State information will be maintained till a final response or a timeout
 - Non-cooperative receivers: State information will be deleted after a timeout or a final response
 - Cooperative receivers
 - ❖ Send non-final response
 - ❖ State information will be held for a longer period
 - ❖ Attack less probable as it requires not only spoofing a sender but also a lot of receivers

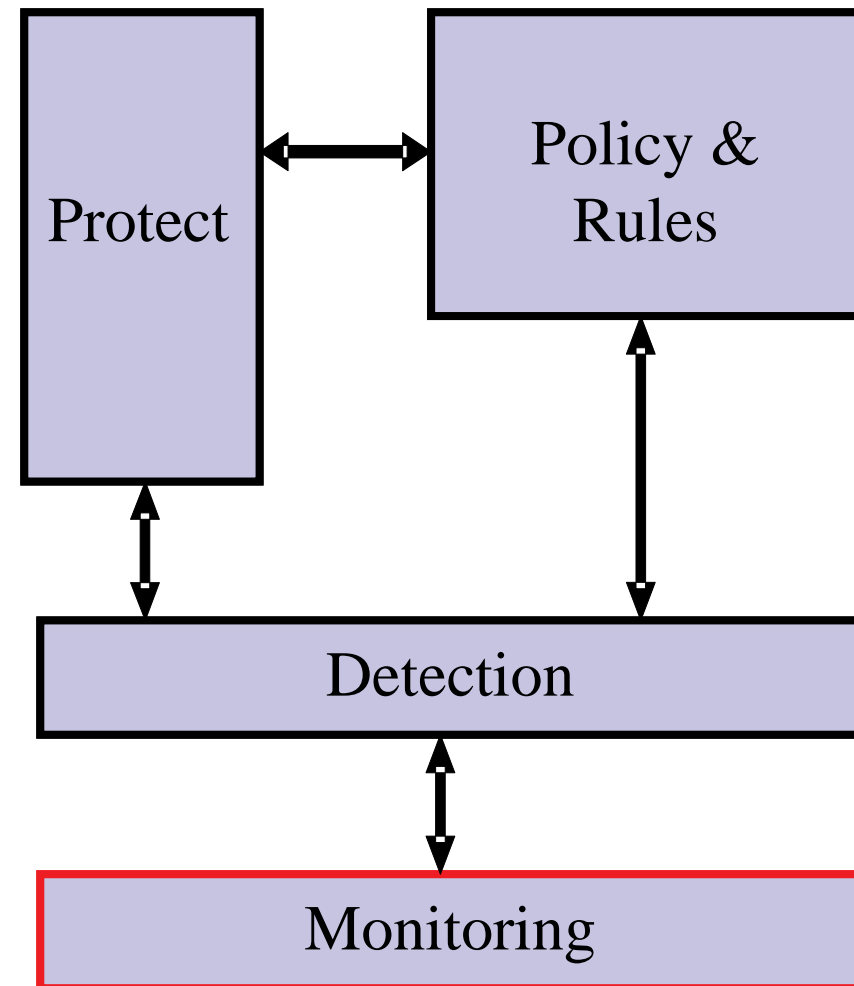
- **Fast**
 - Must process thousands of messages per second
 - Scale with the VoIP infrastructure
- **Non-Intrusive**
 - Do not add delay or SIP headers
 - Do not interfere with NAT traversal or service provisioning
- **Adaptive**
 - Integrate new rules and policies
 - Learn new attack signatures
- **Complete**
 - Analyze message and session irregularities
- **Informative**
 - Provide statistics and alarms in various levels of detail

- Often suggested approach
 - Build an all knowing, all seeing component in front of the SIP proxies
 - This component terminates sessions and starts new sessions to the proxies
 - Controls both signaling and media
 - Provide
 - ❖ Message parsing
 - ❖ Black and white lists
 - ❖ Media screening
 - ❖ Increase QoS

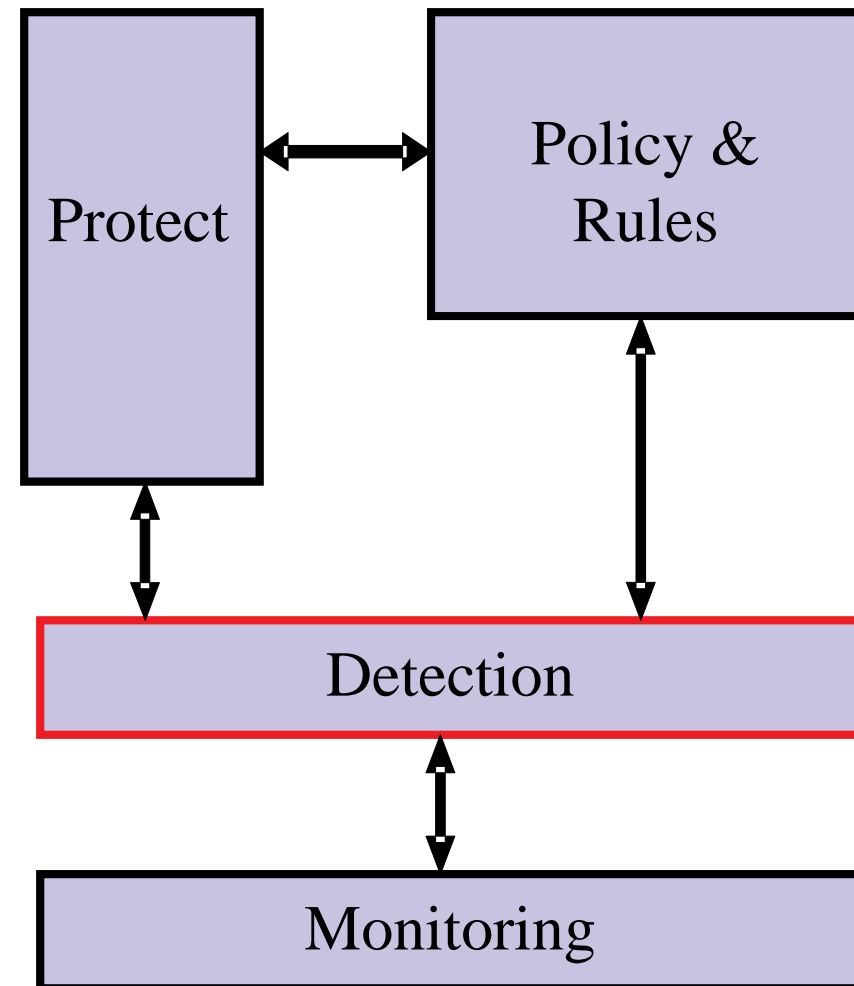


- Solution should be as distributed and scalable as the VoIP infrastructure itself
 - Centralized points are attractive to attack
- Solution should avoid collecting session state
 - Scales only at high hardware costs
 - ❖ SIP Session information can easily reach a few Kbytes
 - Failure would cause session failure
 - ❖ Can only be fixed at even higher costs
- Solution should avoid dealing with media
 - Routing all traffic through a central point increases the bandwidth requirement of the provider considerably
 - No added QoS benefit
 - ❖ In contract, it increases RTT and adds additional processing points

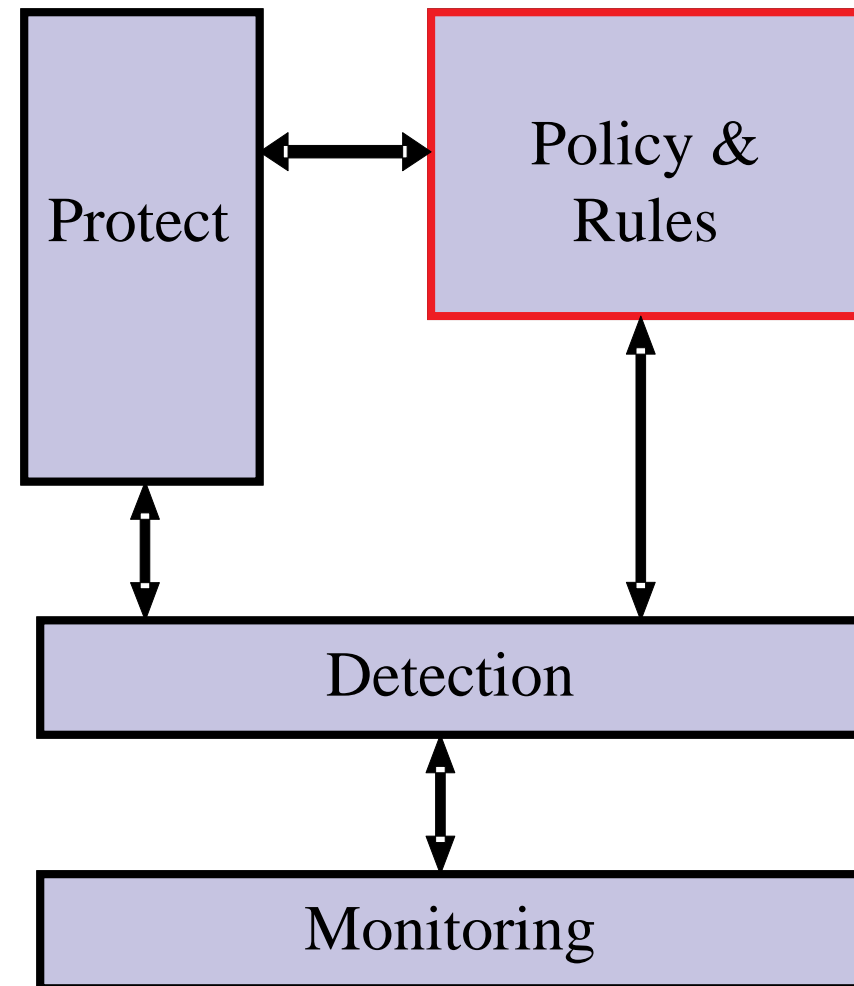
- Monitor and measure incoming traffic
 - Must process thousands of messages per second
 - Work non-intrusively
 - Must not interfere with NAT traversal or the SIP infrastructure itself
 - Adaptive monitoring
 - ❖ Collection and processing is adapted to threat level
 - Apply basic filtering and detection rules
 - Enable off-line detail analysis



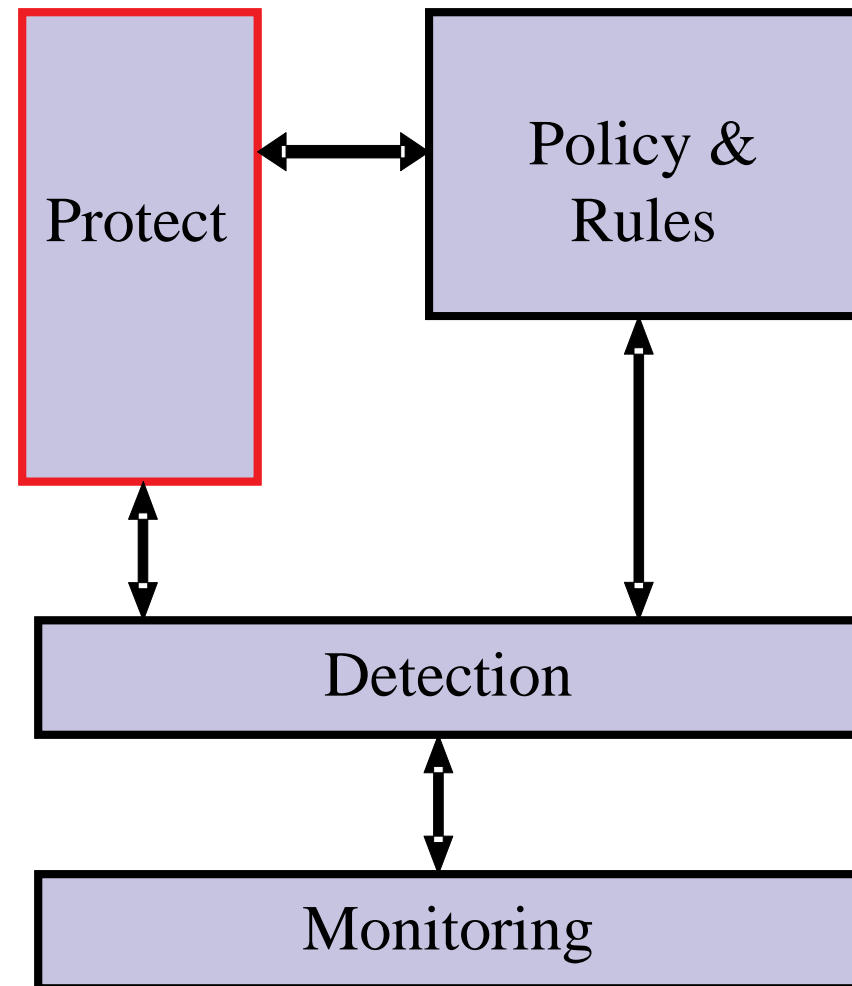
- Identify misbehavior
 - Analyze collected data
 - Apply pre-defined policies
 - ❖ Identify well known signatures
 - ❖ Search for known attacks
 - Apply adaptive rules
 - ❖ Adjust detection thresholds based on changing traffic characteristics
 - Collect information and statistics on
 - ❖ Messages exchanged
 - ❖ Sessions
 - ❖ Failure situations
 - Support different analysis levels
 - ❖ Message based for rapid and on-line detection
 - ❖ Session based (how many sessions were broken, failed ...)



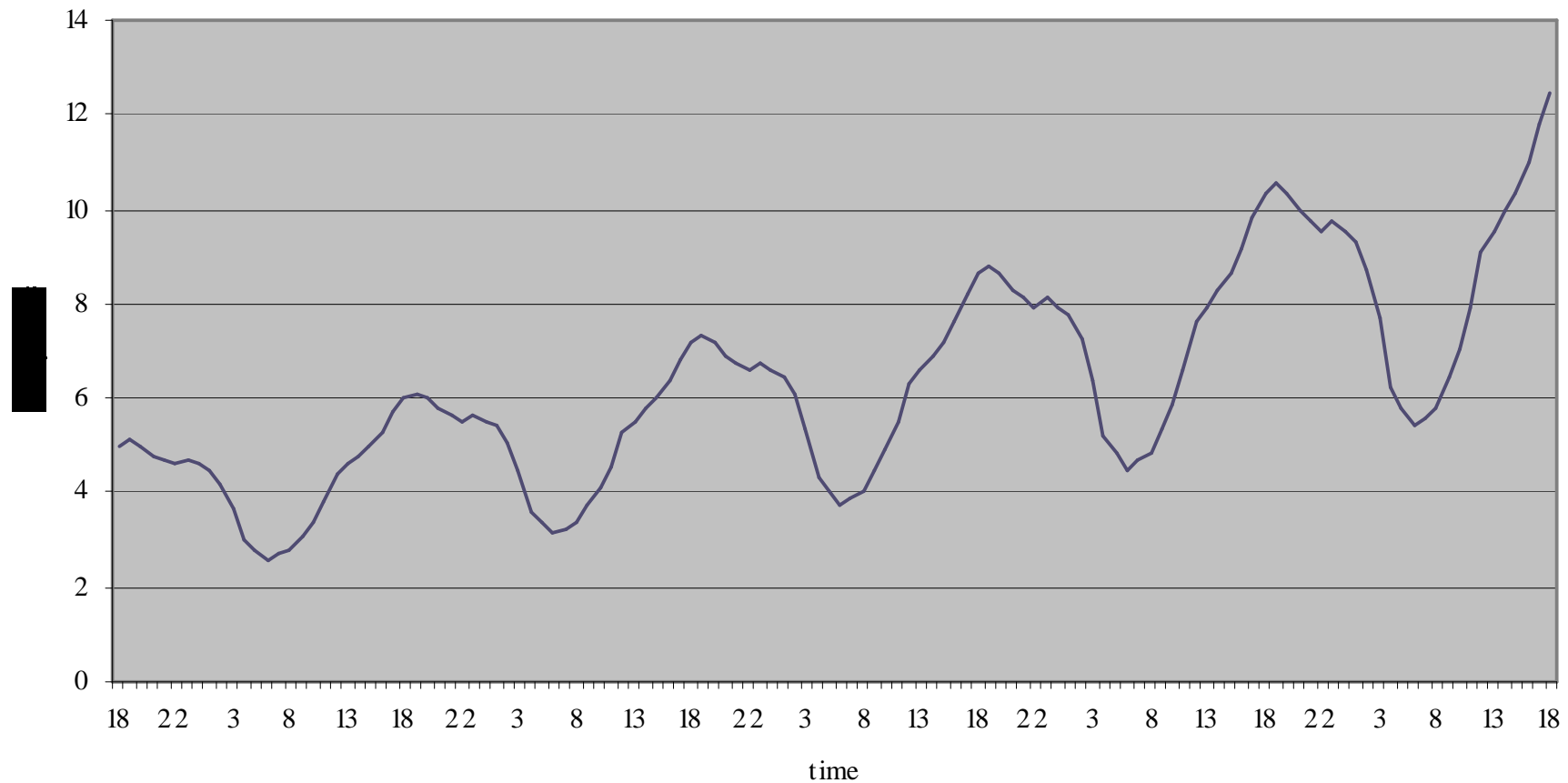
- Allow the specification of
 - Detection signatures
 - ❖ Look for messages with headers in the form of XYZ
 - Policies and rules
 - ❖ Set an alarm when X sessions fail during Y seconds
 - Adaptation rules
 - ❖ If signature A was observed then increase the depth of analysis
 - ❖ Take input from detection component to adjust detection rules



- Protect and alert
 - Combine detection results and pre-defined policies to
 - ❖ Update white and black lists
 - ❖ Generate alarms
 - SMS, Email, flashing lights
 - ❖ Adjust traffic filtering rules

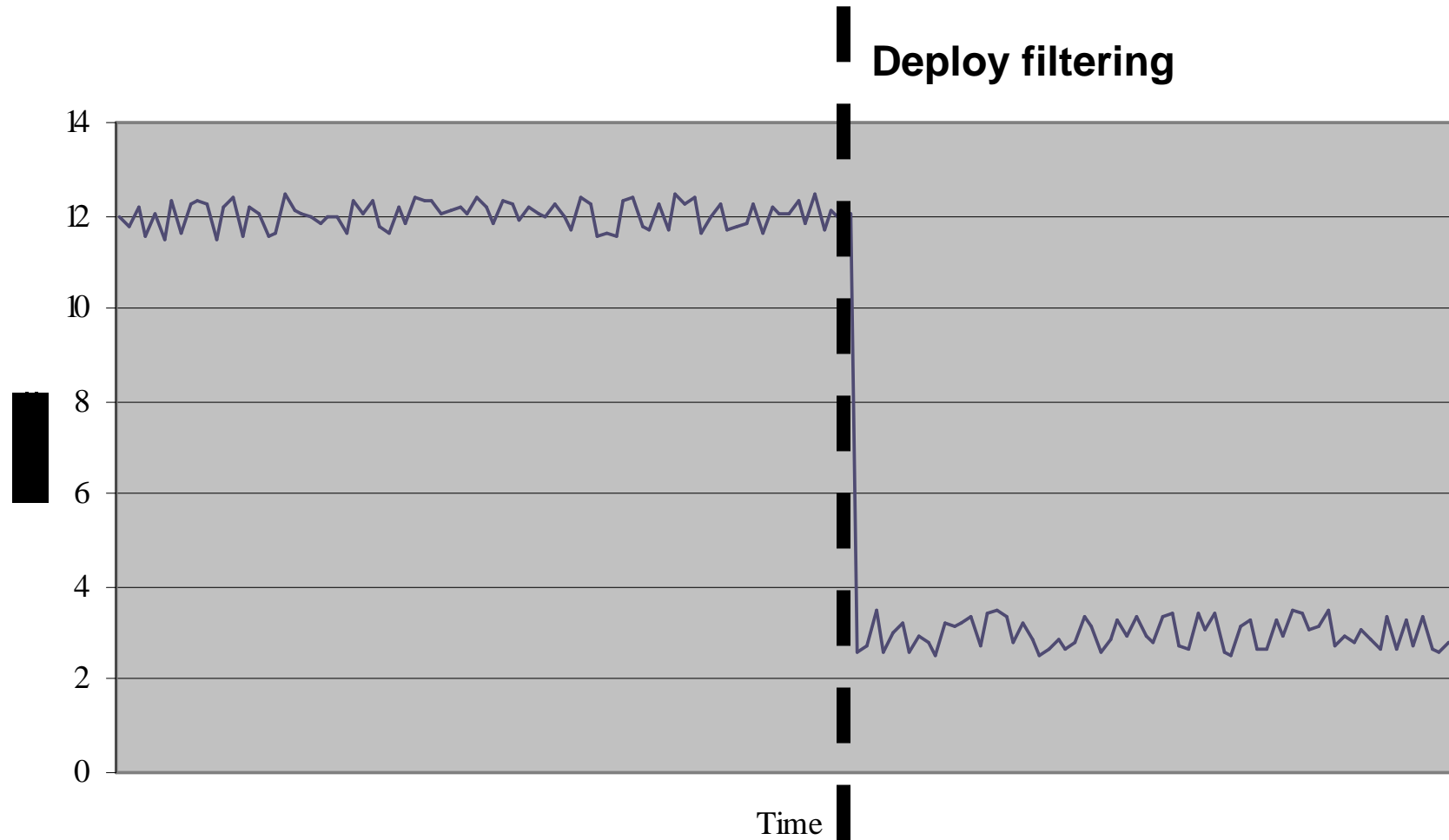


Real Scenario: Traffic Development



- Good sales strategy or is something wrong
- Symptoms
 - Higher load on data bases
 - Higher signaling traffic
 - No significant increase in number of calls
- General traffic analysis
 - No malicious packets
 - Unproportional high number of legal REGISTER messages
- Deep analysis
 - Certain user agents register once a second instead of once an hour
 - User agent otherwise totally RFC3261 conform

- Block all traffic from the IP addresses originating misbehaving traffic
 - Couple SIP logic with IP filtering
 - Possible but
 - ❖ Block all users with misbehaving user agents
- Block all registration traffic from the user agents
 - Simple but
 - ❖ Block all users using the same chip set (chip set indicated as the user agent and not only misbehaving user agents)
 - ❖ Block all users with misbehaving user agents
- Temporarily block registration traffic from the IP addresses generating misbehaving traffic
 - An IP address is misbehaving if it sends more than 3 REGISTER messages in less than one minute
 - If an address is misbehaving then block all REGISTER messages for 1 hour after which three REGISTER messages are allowed



- The enemy is still not the script Kiddy
 - It is those who did not spend enough time to read the RFCs and test their solutions
- DoS detection tools should
 - Recognize changes in traffic patterns
 - Identify misbehaving parties
 - Provide flexible configuration to allow filtering certain traffic
 - They are needed NOW



Thank you for your attention

BTW: we are ALSO hiring ! ;-)

contact@iptego.de