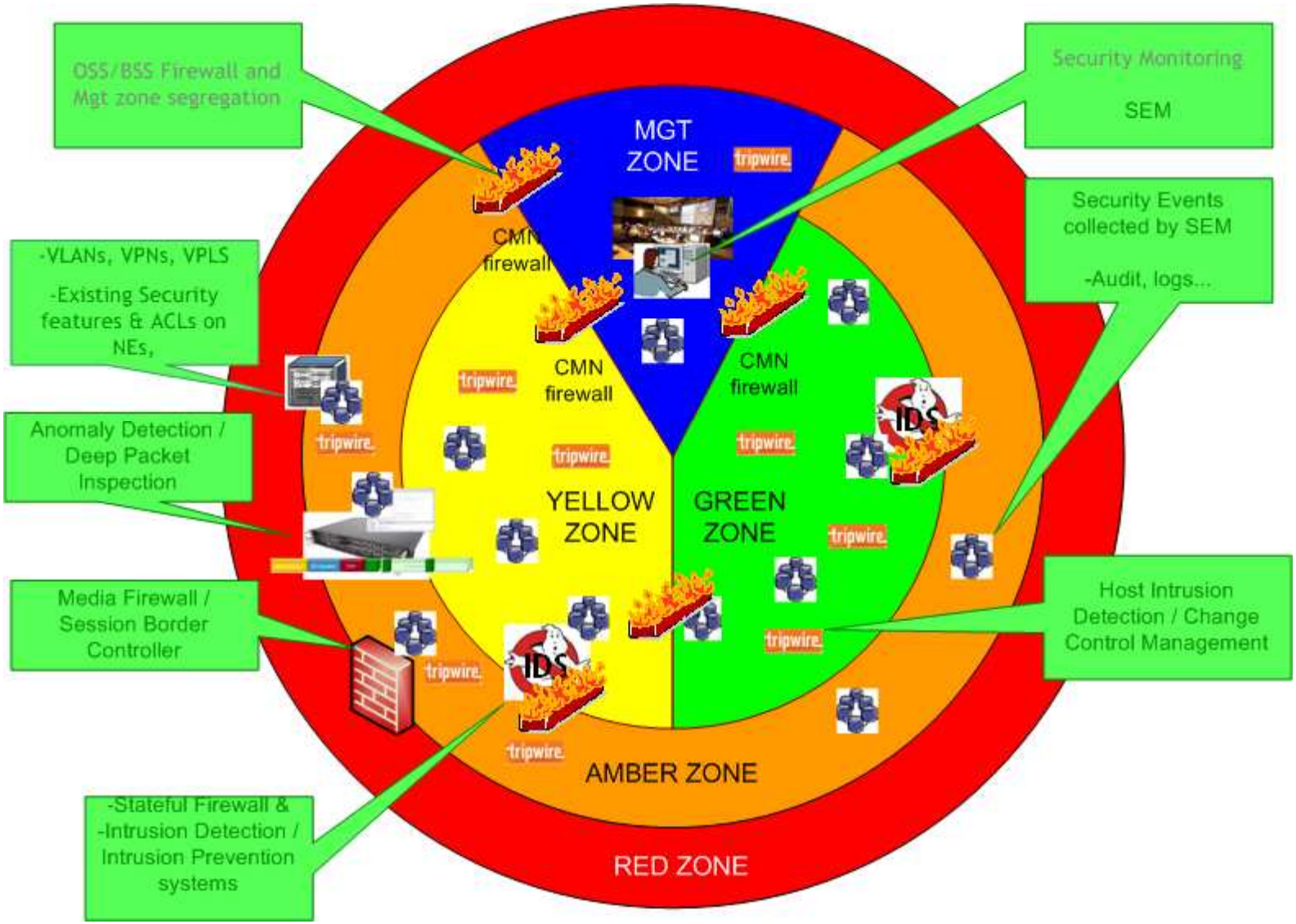
Security Architecture principles

Arnaud Fillette

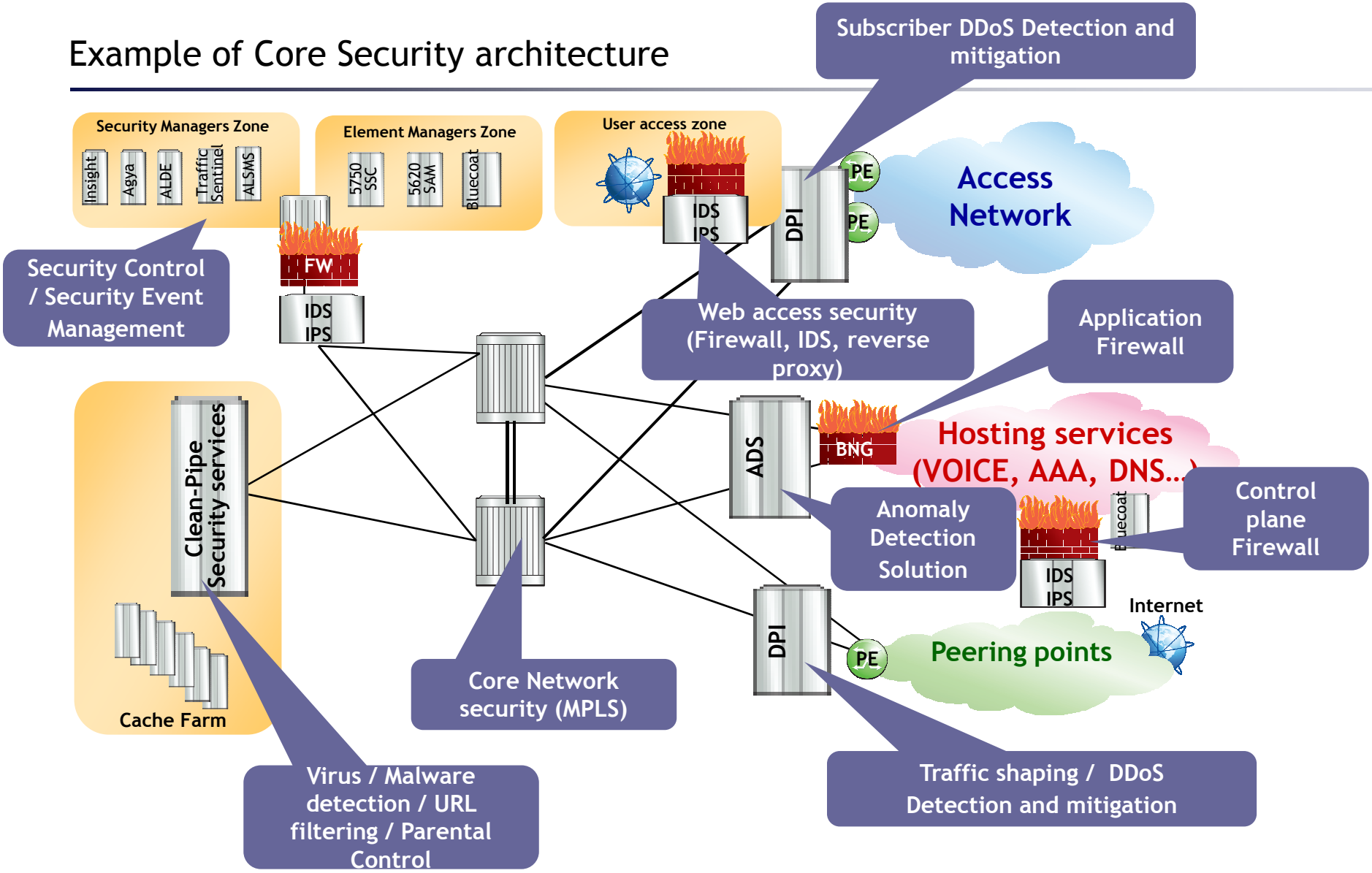
A security design process based on threats / risks analysis and considering customer Security policies

- Segregation of User Plane, Control Plane and Management plane
- Domains (Home user, Access, Core, OSS/BSS..) and Zones (Trusted, Untrusted…) defined considering network flows and CIA requirements (Confidentiality, Integrity, Availability)
- Layer2 / Layer 3 ACLs and VPN/MPLS security for standard segregation on the network
- Physical separate Firewalls to protect Control plane and Management plane
- Application proxies / Reverse proxies in front of Web and Webservices applications
- Detection solutions where relevant (Anomaly detection / IDS / IPS)
- Value-add security services for services providers (traffic management, Clean-pipe malware/virus detection, URL filtering)
- Hardening of Network elements and element managers according to Best practices (CIS benchmarks, ALU security guidelines…)

Design – Security Architecture Concepts

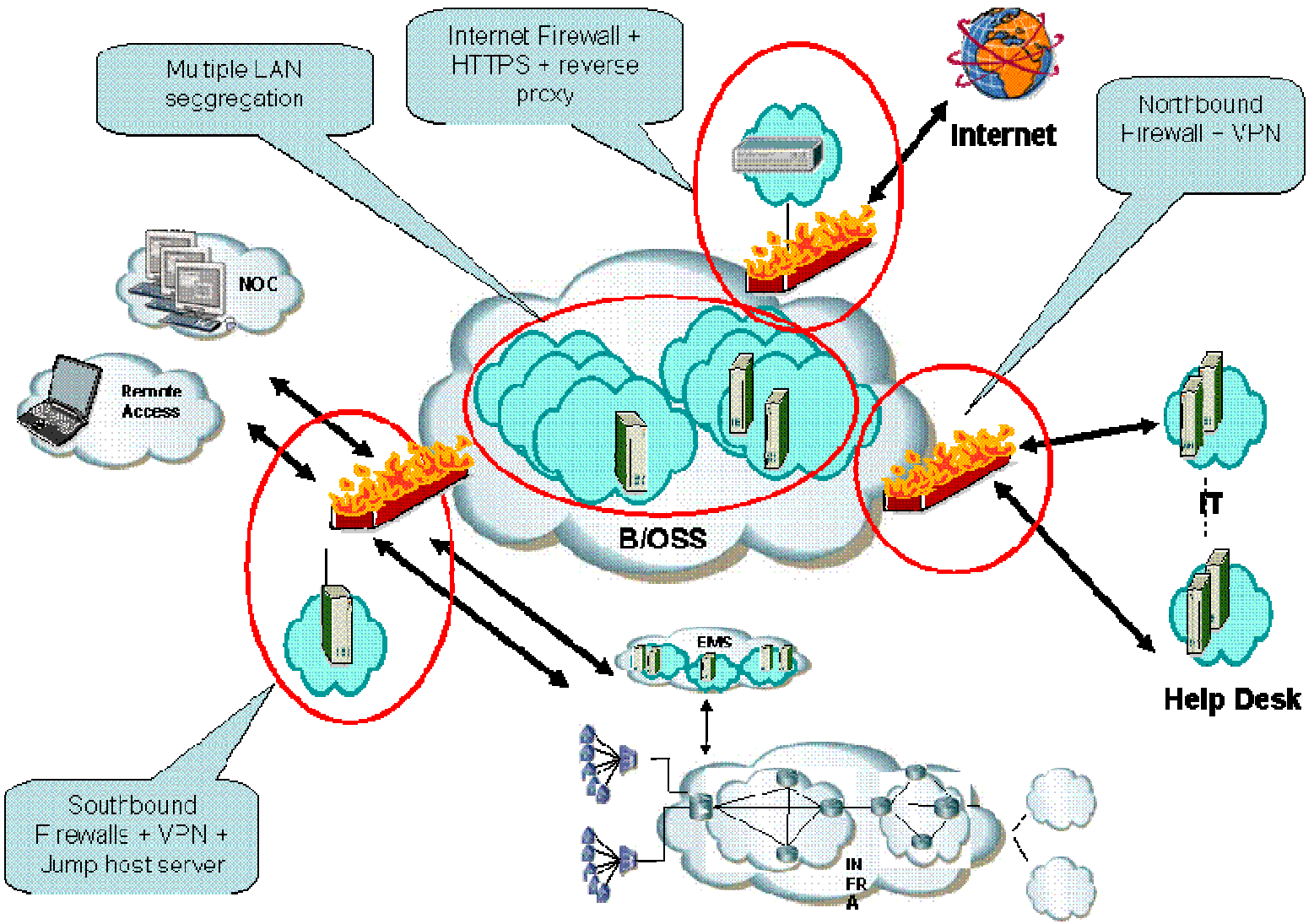


Example of Core Security architecture



Alcatel·Lucent

OSS / BSS Security – Reference Design



Alcatel·Lucent

Protecting the Core network / MPLS security

MPLS is not better or worst than any other technology. It just requires to follow good design principles

- MPLS
  - Is a layer 2 switching technology offering VPN functionality for traffic separation
  - Requires a strong protection of the Core network
  - Does not replace any other security solution to guarantee the confidentiality and integrity of customer Data (IPSec VPN…)
- The threats
  - Label info disclosure / label enumeration (A way to get information about how the network is built)
  - Rogue path switching / rogue destination switching (To be able to inject traffic and compromise the switching mechanism)
  - Label info poisoning / DoS (To modify the integrity and availability of the network)
- High level Recommendations
  - IP/application authentication and encryption (IPSeC VPN, HTTPS, SIP-S)
  - Authentication and integrity checking (MD5) to accept LDP updates for trustworthy sources only
  - Security Monitoring and health checking of network devices to track any changes and availability issues on the network

Protecting the Core network / MPLS security

MPLS is not better or worst than any other technology. It just requires to follow good design principles

- MPLS Design rules
  - Static routing between PE and CE (protect against routing protocol attacks)
  - Spoofing protections (dropping labeled packets from CE / VRF segregation)
  - Controlling access to devices (AAA)
  - Controlling changes (configuration integrity checking / change control mgt)
  - ACLs to restrict routing traffic to the peering interface (when not static)
  - CEs and PEs on different VLANs and different physical switches
  - Use of firewalls on peering points (VPN connected to the Internet)
  - CE router managed by Provider
- The role of a Security Information & Event Management Solution (SIEM)
  - No specific Security detection solution at this level of the network
  - Information provided by the network elements and test tools are usually enough to trigger potential security breaches
  - The SIEM will be able to correlate different information from various place of the network
  - The response to an attack needs be designed appropriately (pre-plans)

Protecting the Core network / controlling the customer traffic

Traffic shaping / DoS and DDoS detection / Anomaly detection / Virus and Malwares protection

- DPI solutions provide ability to offer higher value security services to customers
  - SLA guarantees to customers (e.g. hosted platforms, businesses)
  - Provides wire speed DoS/DDoS, worms and Botnet detection
  - Anomaly detection (heuristics algorithms)
  - Layer 3 to Layer 7 protocol analysis
  - Expandable with new applications – LI, spam/phishing control
  - Reduces OPEX - Less operations time spent resolving customer issues e.g. DDoS attacks
  - Reduces CAPEX – network resources not consumed by spurious traffic
  - Maintains and/or improves customer satisfaction
- Traffic Management and DPI solutions can be used to redirect specific customer traffic to associate the appropriate treatment (User traffic control solutions)
  - Malware / Virus detection (Payload analysis)
  - Web caching
  - URL filtering (white-list / Black-list / Parental control)

Protecting the Core services of the NGN infrastructure

Lots of services requiring specific attention (DNS, NTP, AAA, VOIP services…)

- Media Firewalls and specific detection solutions
  - Media Firewalls (BNG…) to provide the VOIP application NAT and topology hiding
  - Specific Anomaly Detection solutions to detect abnormal behaviour of signalling flaws and Media flaws (SIP attacks, RTP/RTCP attacks…)
- Standard Firewalls + IDS/IPS on the control plane
  - Traditional tiered approach – (Network-IPS-FW-Application)
  - Firewall applies/enforces traffic policies
  - IDS/IPS monitors traffic to detect known and anomalous security events
  - IDS/IPS Alerts and protects against identified security events
  - Key goals are to improve ***reliability*** and ***availability*** of protected elements
  - Key benefit – ***Helps service provider to manage risks***
- The role of a Security Information & Event Management Solution (SIEM)
  - Correlates the information from the various filtering and detection solution
  - Provides appropriate events to trigger the decision (when an automatic response is not designed / i.e. IPS solutions)
  - Provides the required level of reporting to monitor the security health of the network and services

Protecting the Management layers

Avoiding the risks of attacks from 3rd parties and controlling changes

- Southbound and Northbound Firewalls to guarantee OSS and BSS segregation
- Secured Management access solutions
  - Centralized authentication, SSO, AAA
  - JumpHost, Secured remote access (VPN Gateways)
- Reverse Proxies and Application control
  - XML proxy for Webservices security control
- Change Control
  - Security Event Management to monitor access and Security logs
  - HIDS and Change Control Management solutions

www.alcatel-lucent.com