Sichere Infrastrukturen
mit HP's Adaptive Network Architecture

Holger Rank
HP Services
ANA EMEA Sales
holger.rank@hp.com

Agenda

- Security Ausgangslage
- Anforderungen und Problemstellungen an ein sicheres Netzwerk und IT-Infrastruktur
- Security Lösungen inkl.
  - Netzwerk + IT
  - Security + Incident Management
  - Beispiele aus der Praxis
- Gesamtüberblick

Agenda

- **Security Ausgangslage**
- Anforderungen und Problemstellungen an ein sicheres Netzwerk und IT-Infrastruktur
- Security Lösungen inkl.
  - Netzwerk + IT
  - Security + Incident Management
  - Beispiele aus der Praxis
- Gesamtüberblick

Security Ausgangslage (1/2)

- Historisch gewachsene IT Infrastruktur
- Hohe Anforderungen an die Verfügbarkeit
- Starker Kostendruck – IT muss Kosten einsparen!
- Sicherheit kaum vorhanden
- Unternehmens-Sicherheitsbeauftragter nicht vorhanden
- Unternehmens-Sicherheitsstrategie nicht vorhanden
- Betriebs- und Sicherheitskonzepte, wenn vorhanden meist in einem „Kopf“
- Keine ganzheitliche Sicherheitsbetrachtung der IT Infrastruktur und Liegenschaften
- Keine Schutzbedarfsfeststellung und Risikobetrachtung vorhanden

Security Ausgangslage (2/2)

- Sicherheitsanforderungen durch den Gesetzgeber
  - Datenschutzgesetz
  - KontraG
  - Basel II
- Forderung nach Sicherheitszertifikate
  - BSI Zertifikat
  - BS7799 / ISO17799 Zertifikat
- Vermehrt Werksspionage – das neue Produkt
- 11. September und die Nachwirkungen
  - U.S. Department of Homeland Security
  - Backdoors
  - Überwachung

Agenda

- Security Ausgangslage
- **Anforderungen und Problemstellungen an ein sicheres Netzwerk und IT-Infrastruktur**
- Security Lösungen inkl.
  - Netzwerk + IT
  - Security + Incident Management
  - Beispiele aus der Praxis
- Gesamtüberblick

Anforderungen und Problemstellungen
an ein sicheres Netzwerk und IT-Infrastruktur (1/3)

- Unternehmensweite Security Strategy / Policy
- Erfassung aller IT-Systeme und Anwendungen
- Schutzbedarfsfeststellung und Risikoanalyse inkl. Feststellung der Anforderungen an die:
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
- Erstellung / Einführung sicherer Schutzmaßnahmen
- Dokumentation der Schutzmaßnahmen
- Personal
  - Sicherheitsbeauftragter
  - Security Spezialist
  - Security Incident Response Team

Anforderungen und Problemstellungen
an ein sicheres Netzwerk und IT-Infrastruktur (2/3)

- Zentrales Security Management
- Transparenter Aufbau der Netzwerk und IT Infrastruktur
  - Fokus auf Business und Security Anforderungen
  - Kosteneinsparung
  - Optimierung der Aufwände (Umfang und Zeit) für Änderungen und Erweiterungen
  - Flexible Integration von internen und externen Abteilungen, Partnern, Dienstleister, Zulieferer, neue Tochterfirmen usw. sowie deren Abtrennung
  - Virtualisierung des Netzwerkes
  - Optimierung der Prozesse
- Sanfte und businessorientierte Migration zur sicheren Netzwerk und IT-Infrastruktur

Anforderungen und Problemstellungen
an ein sicheres Netzwerk und IT-Infrastruktur (2/3)

- Company weit einheitlich Security Regeln / Policies
- Funktionierendes Service und Betriebskonzept
- Integration neuer Technologien wie
  - Wireless LAN und dessen Security
  - Anbindung des Produktionsnetzwerkes an das normale Kunden Hausnetz
  - Einführung zentraler Rechtevergabe/-verwaltung über Directories (AD, eDirectory usw.) und 802.1X

Ein gutes und sicheres Gefühl alles notwendige getan zu haben

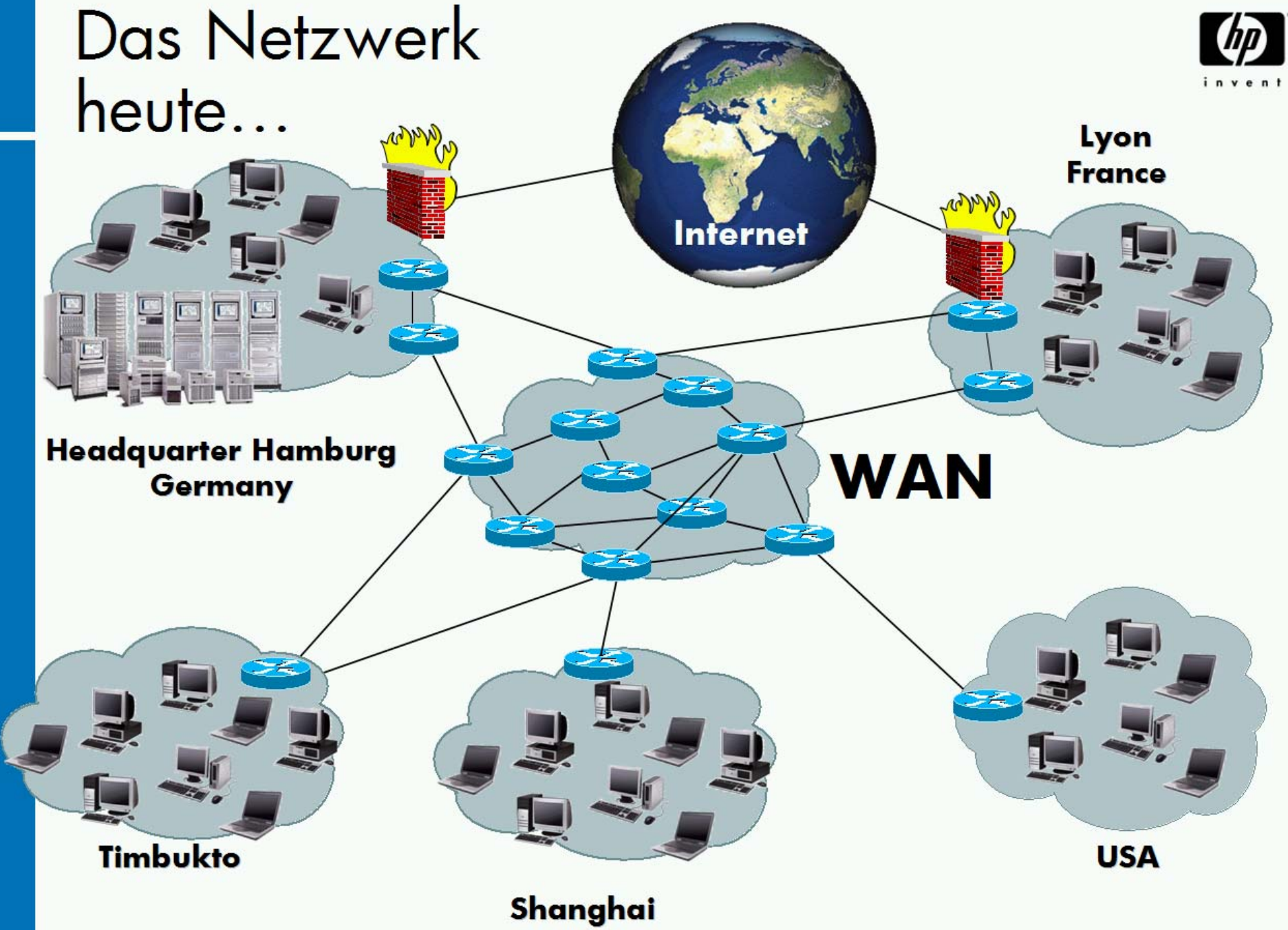
Agenda

- HP NSG Vorstellung
- Security Ausgangslage
- Anforderungen und Problemstellungen an eine sichere Netzwerk und IT Infrastruktur
- **Security Lösungen inkl.**
  - Netzwerk + IT
  - Security + Incident Management
  - Beispiele aus der Praxis
- Gesamtüberblick

Security Lösungen

- Möglichst Standards einsetzen
  - Leichtere Konfiguration und Betrieb
  - Vielfältiger Support
  - Sicherheitslücken werden schneller behoben
  - Möglichst „Boxed“ Lösungen – erleichtert den Support!
  - Homogene Security Infrastruktur – sonst kein durchgehendes Management
- Betrieb und Überwachung
  - Zentrales Management für die gesamte Sicherheitstechnik und relevanten IT-Systeme
  - durch eigenen Fachabteilung
  - durch Servicepartner wie HP Services
  - Eingreifplan bei Incidents

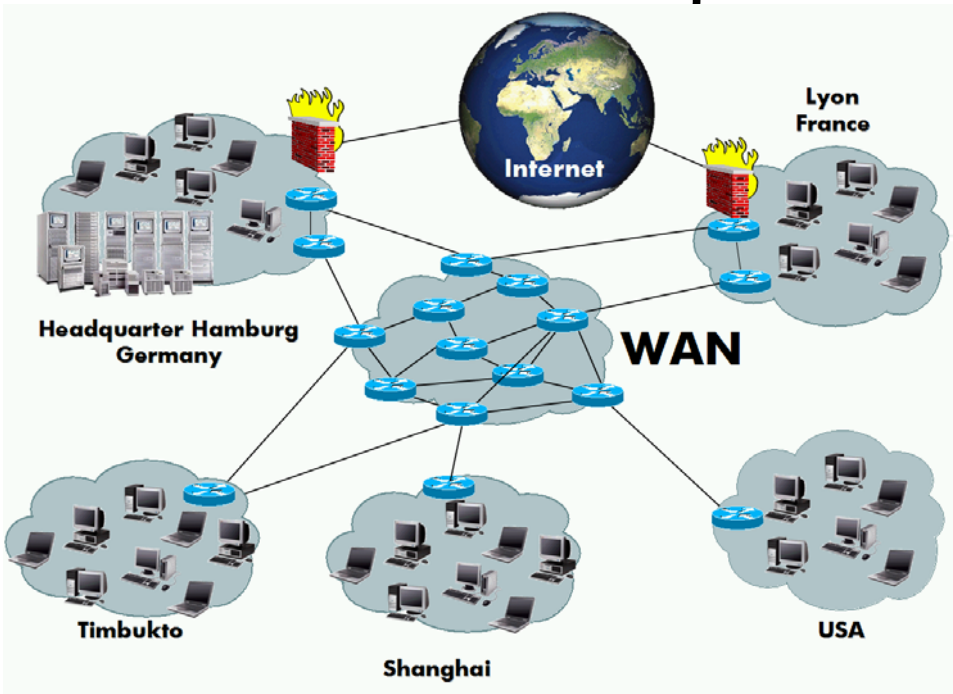
Das Netzwerk heute…

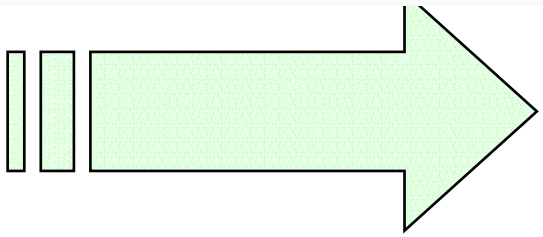


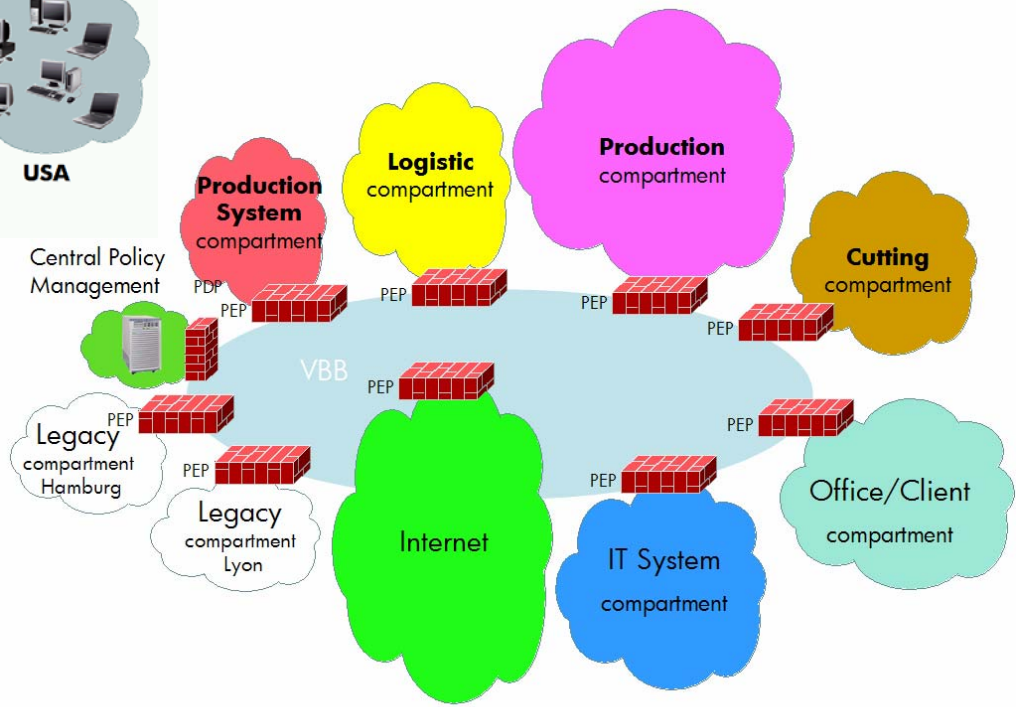
Die Steps zu einem sicheren Netzwerk

1. Aufbau und Implementierung einer Security Strategy
2. Strukturierung der IT nach Business- und Sicherheitsbedarf
3. Festlegen der Sicherheitsmaßnahmen
4. Erstellen von Policies bzw. Standards für die einzelnen Bereiche / Compartments
5. Aufbau eines zentralen Managements
6. Schrittweise Migration zur neuen Netzwerk und IT Struktur
7. Daily Business: mit dem sicheren und flexiblen Netzwerk und der IT Infrastruktur

Restrukturierung des Netzwerkes







Festlegen der Sicherheitsmaßnahmen

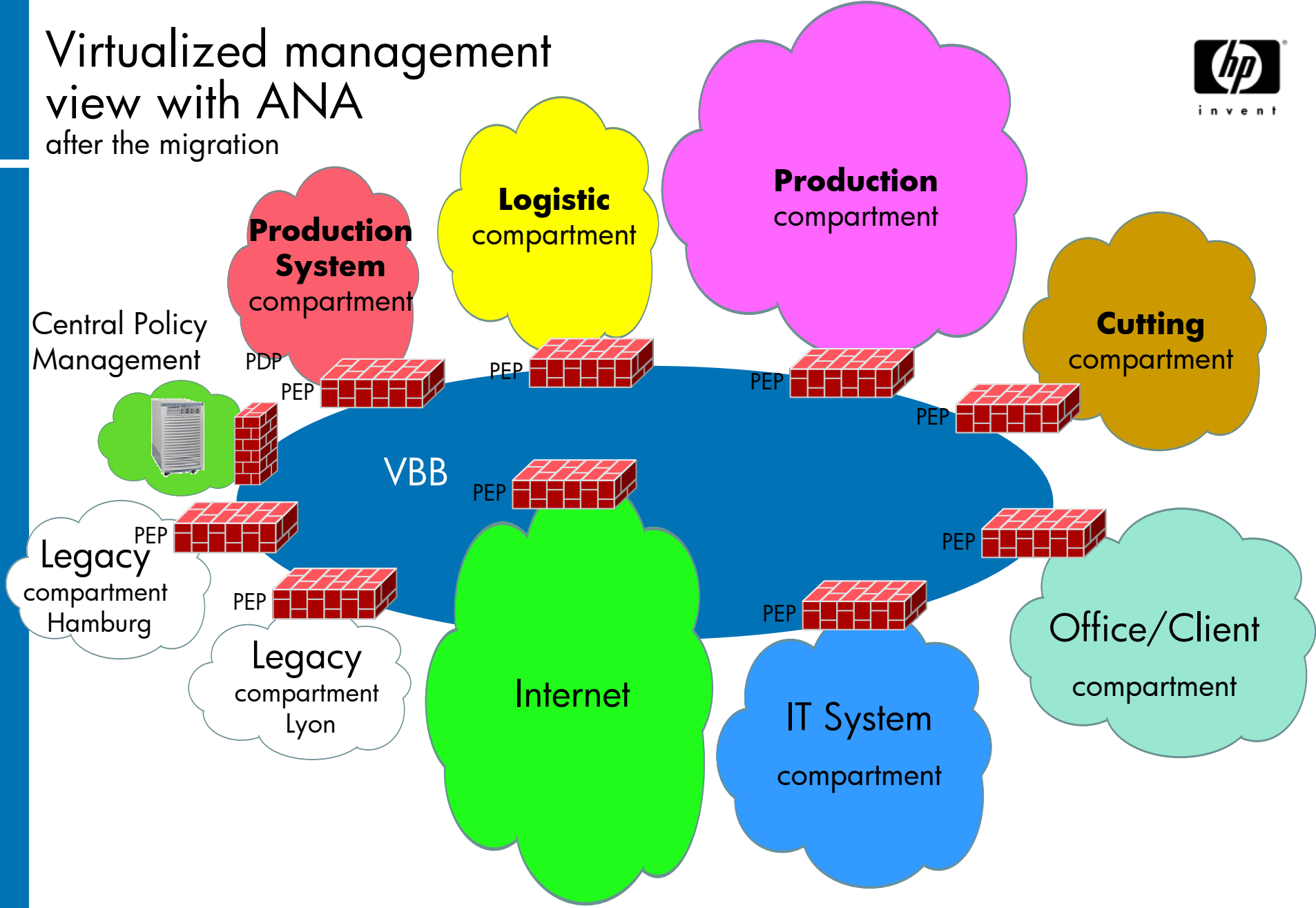
- Kontrollinstanzen
  - Router mit Access Listen
  - Switches mit Access Listen
  - Paketfilter
  - Stateful Inspection Firewalls
  - Proxy Firewalls
  - 802.1x / IBNS
- Benutzer + Rechte Verwaltung
  - Active Directory oder andere Directories (LDAP, eDirectory)
  - Radius
  - Passwort
  - Smardcards + Token
  - MAC und IP Adressen

Festlegen der Sicherheitsmaßnahmen

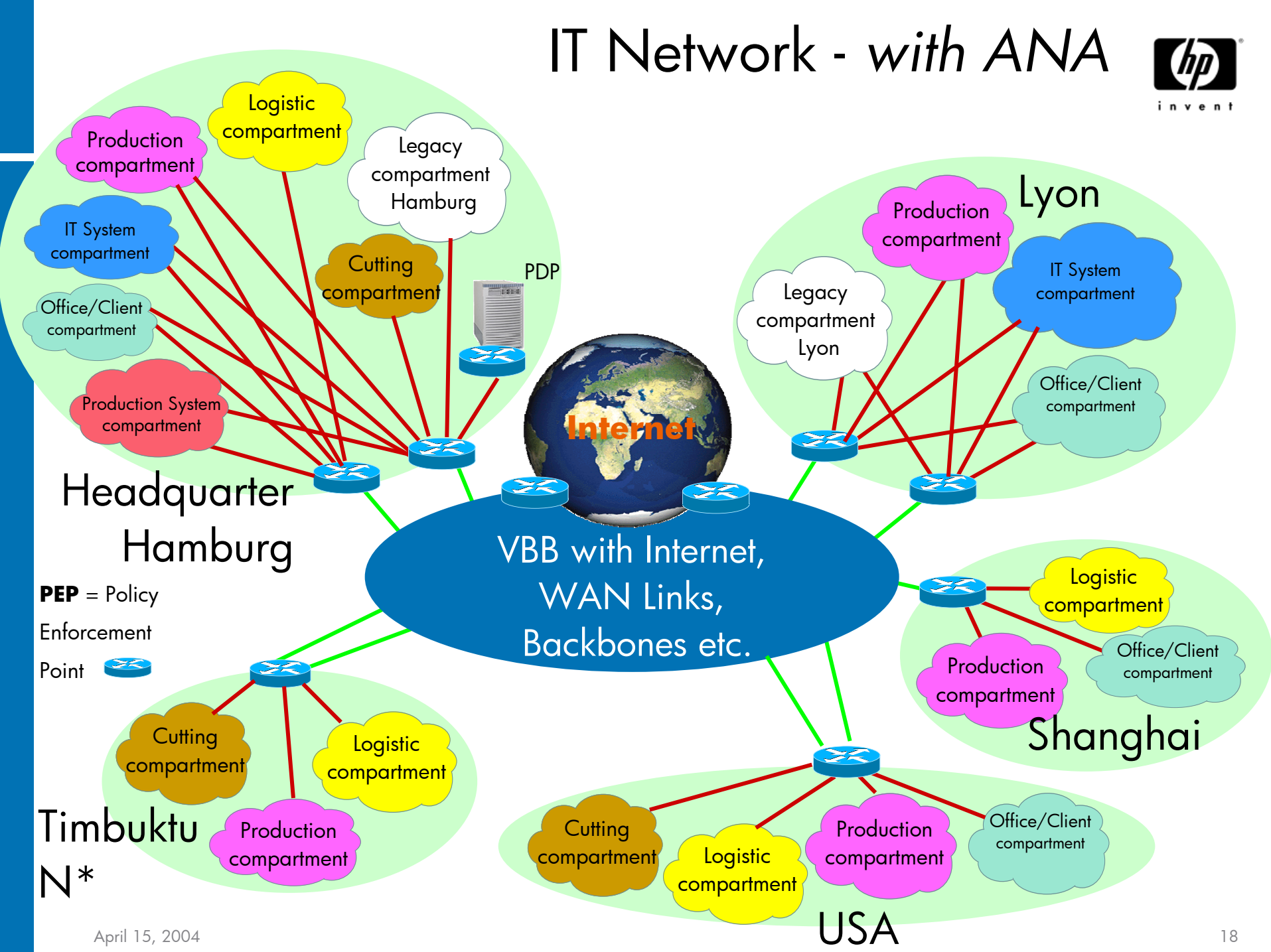
- Device Security
  - Virenscanner, Personal Firewalls, Encryption, Smartcards
  - Wirkliche Rechtevergabe für Access und Filezugriff lokal + remote
  - Backup & Recovery
- Systemüberwachung
  - Network Intrusion Detection Systeme
  - Host Intrusion Detection Systeme
  - Logfile Auswertung
- System Management
  - End-to-End Management für alle Komponeten
  - Flexible Nutzung vorgefertigter Maßnahmen
  - Konsolidierte Darstellung und Auswertung von Logs (IDS, Hosts, Firewalls)
  - Incident + Troubleticket Management
- Erstellen der einzelnen Policies

Virtualized management view with ANA

after the migration

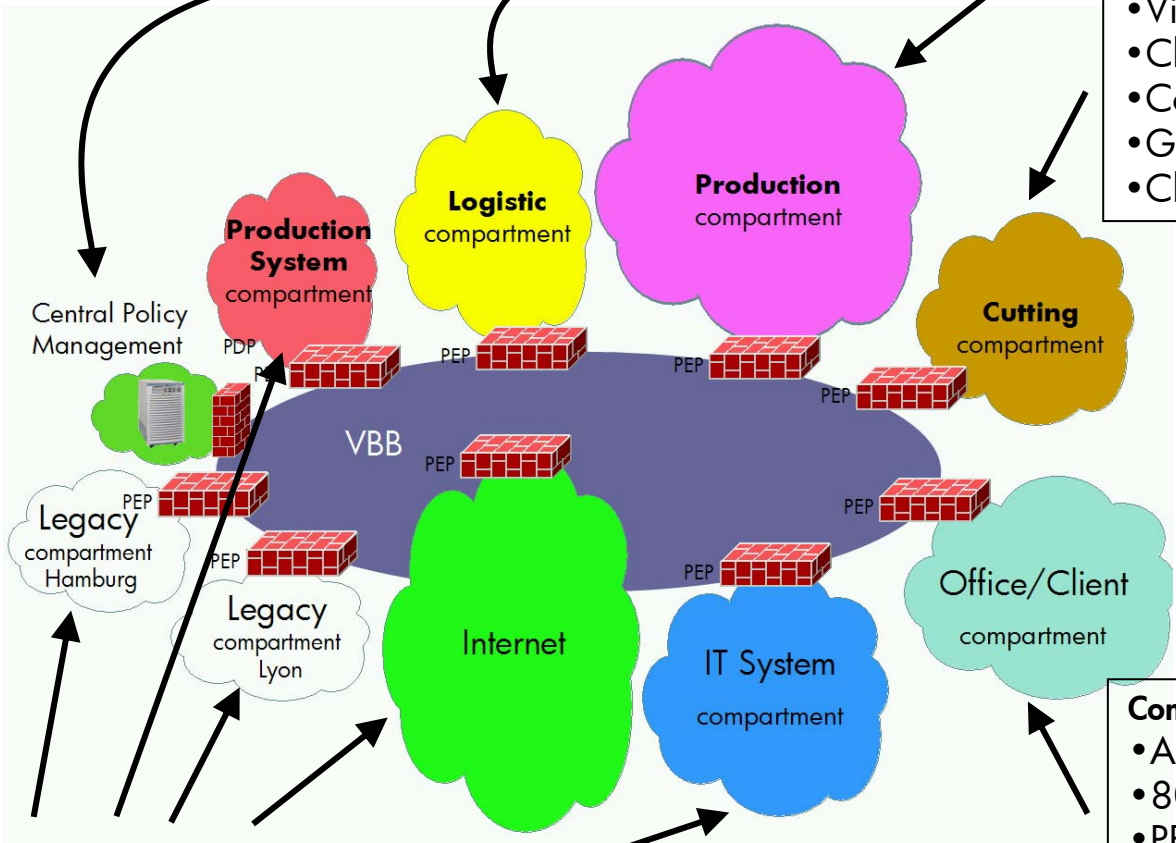


IT Network - *with ANA*



Virtualized management view with ANA & Security Solution's

after the migration

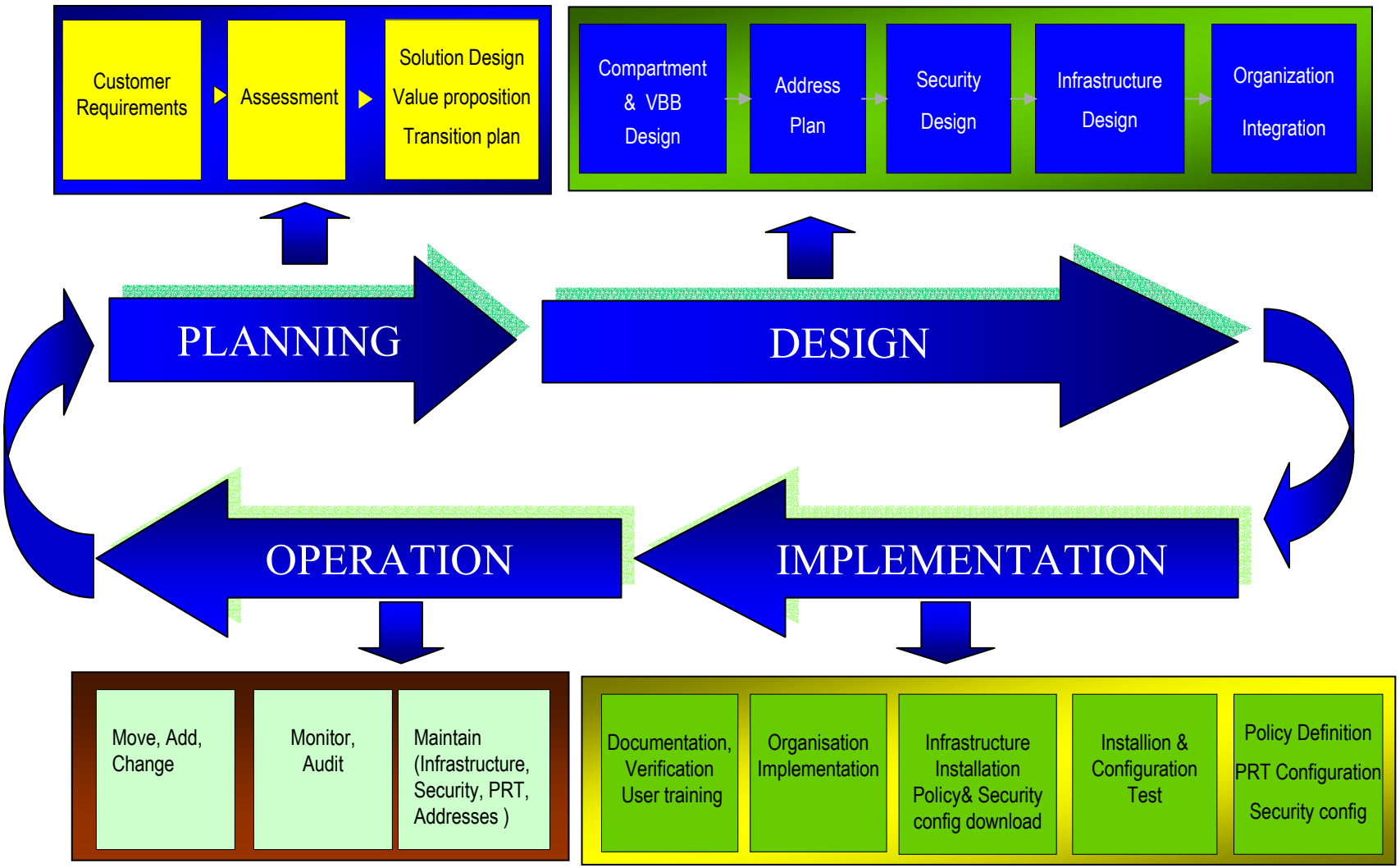


Compartment Security usage:
- ANA
- 802.1x / IBNS
- PEP's Router/Switches/Firewall
- IDS
- Virus&Content Protection
- Client preScan
- Content Scanning
- Guest LAN
- Client Isolation

Compartment Security usage:
- ANA
- PEP's Router/Switches/Firewall
- IDS
- Virus&Content Protection
- Directory integration

Compartment Security usage:
- ANA
- 802.1x / IBNS
- PEP's Router/Switches/Firewall
- IDS
- Virus Protection
- Client preScan
- Directory integration
- Single Sign On
- Personal Firewall

ANA Methodology



Agenda

- HP NSG Vorstellung
- Security Ausgangslage
- Anforderungen und Problemstellungen an eine sichere Netzwerk und IT Infrastruktur
- Security Lösungen inkl.
  - Netzwerk + IT
  - Security + Incident Management
  - Beispiele aus der Praxis
- **Gesamtüberblick**

Gesamtbild

- Einfache flexible Security Lösung auf Basis von ANA
- Unternehmensweite Security und IT Policy
- Zentrales Security und IT Management
- Starke Visualisierung der IT Infrastruktur durch ANA
- Visualisierung nach Business und Security Anforderungen!
- Schnelle Implementierung und Änderungen möglich
- Keine Nebenwirkungen bei Änderungen/Erweiterungen für benachbarte Bereiche
- Anbindung und Absicherung selbst problematischer Bereiche wie Industrial Ethernet Produktionsstätten an die normale IT Infrastruktur
- HP benutzt ANA seit über 3 Jahren für die eigene IT (Aufwände zu Implementierung bei HP ca. 2/3 der jährlichen Einsparungssumme!)
- HP hat 5 Patente für ANA

Gesamtbild

Schritte zu einer sicheren IT Infrastruktur:

1. Aufbau+Rollout einer unternehmensweiten ANA Security Strategy
2. Implementierung der notwendigen Security Rollen/Funktionen
3. Implementierung der Security-Policies und –Prozesse mit ANA
4. Ist-Aufnahme der aktuellen IT und ggf. Infrastruktur
5. Schutzbedarfs- und Risikofeststellung Ongoing
6. Planung + Einführung von weiteren Security Maßnahmen
7. Daily Business (selbst oder über z.B. HP Services)
8. Regelmäßige Security Reviews (min 1x/Jahr)

Gesamtbild durch HP Security Services mit ANA

Ergebnis:

Ihr Unternehmen ist sicher!

Kleine Anmerkung: 100%tigen Schutz gibt es nicht ☺


invent