Vers un nouveau modèle de sécurisation

Le « Self-Defending Network »

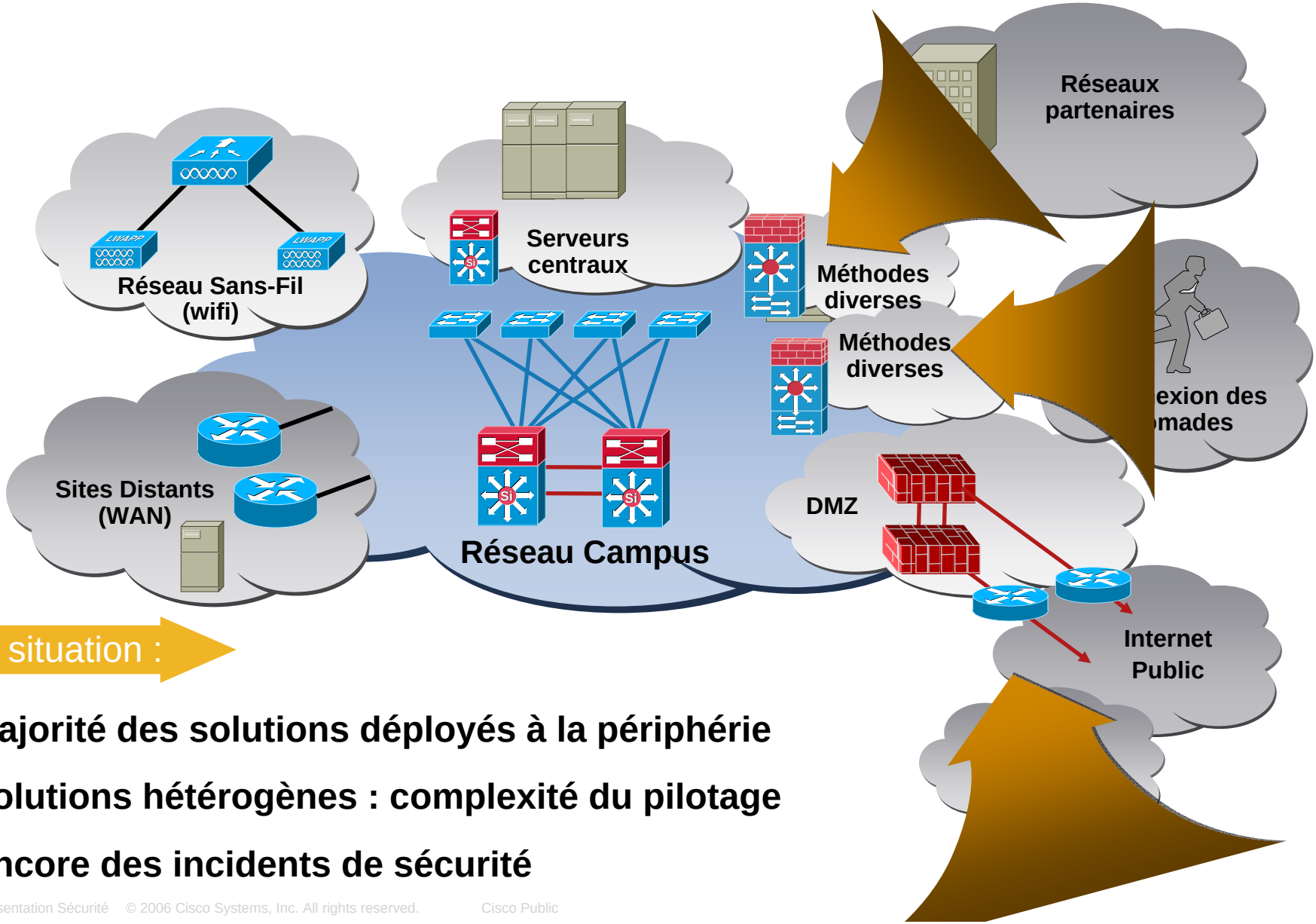
Conférence Annuelle Avril 2009 – Network Academy

Babacar Wagne – bawagne@cisco.com -- Responsable Technique du segment Commercial & Entreprises Afrique de l'Ouest et Centrale.

Agenda

- Stratégie de sécurité Cisco :
  - Le self-defending network
- Gamme de solutions
- Mise en application

La vision actuelle de la sécurité



La situation :

- **Majorité des solutions déployés à la périphérie**
- **Solutions hétérogènes : complexité du pilotage**
- **Encore des incidents de sécurité**

Un environnement ouvert, des défis complexes

De nouvelles menaces

- Erosion du périmètre
- SPAM / Malware / Recherche de profit
- Perte et fuite d'information

Collaboration et Communication

- Mobilité Interne et externe
- Accueil des visiteurs, des partenaires
- Outils de collaboration : TéléPrésence/ Vidéo / IM / Web 2.0

L'impact business

- Stratégie de gestion des risques IT
- Conformité aux normes et réglementations
- La sécurité comme moteur de l'innovation
- Contrôle des coûts

L'information à protéger est distribuée et mobile, la sécurité doit s'adapter

Le besoin de solutions de sécurité

Conformité

Fuite d'information

Une approche système est nécessaire pour rationnaliser la gestion des risques IT

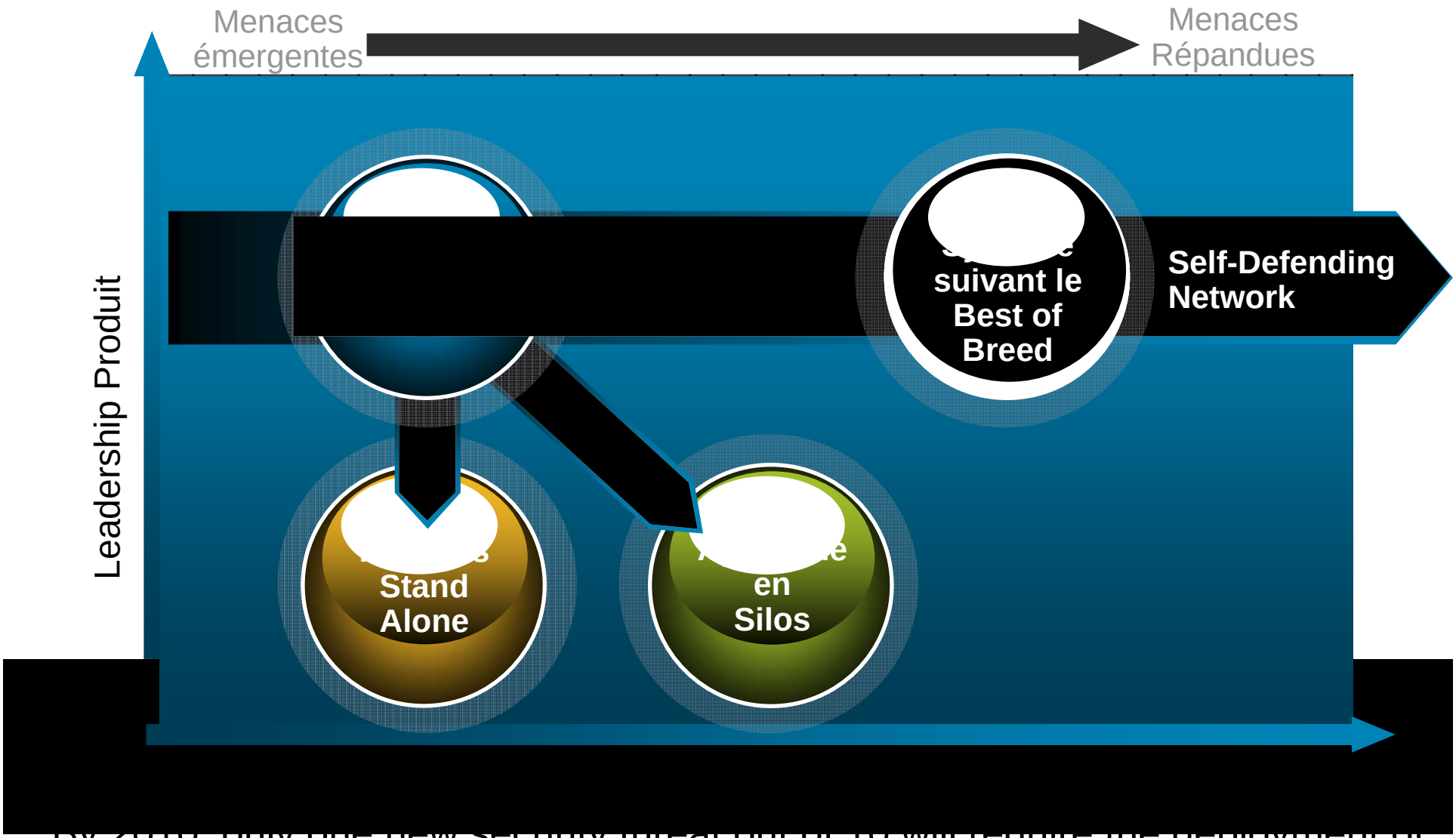
Gestion des menaces

Identité, sécurisation interne

Solutions de Sécurité Cisco

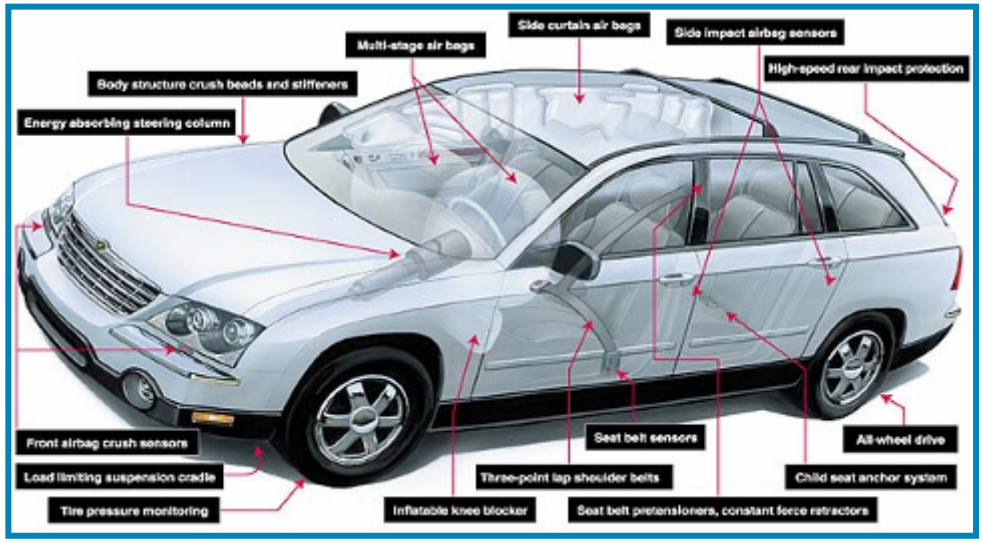
- Intègre des fonctions de protection du poste, du réseau, du contenu, et des applications pour bloquer les menaces
- Protège des dernières menaces, en utilisant des informations récoltées globalement à l’échelle d’internet.
- Fournit une protection end-to-end, avec une approche de défense en

Du Best-of-Breed à l'approche système



By 2010, only one new security threat out of 10 will require the deployment of a tactical point solution, compared with eight out of 10 in 2005." **Gartner**

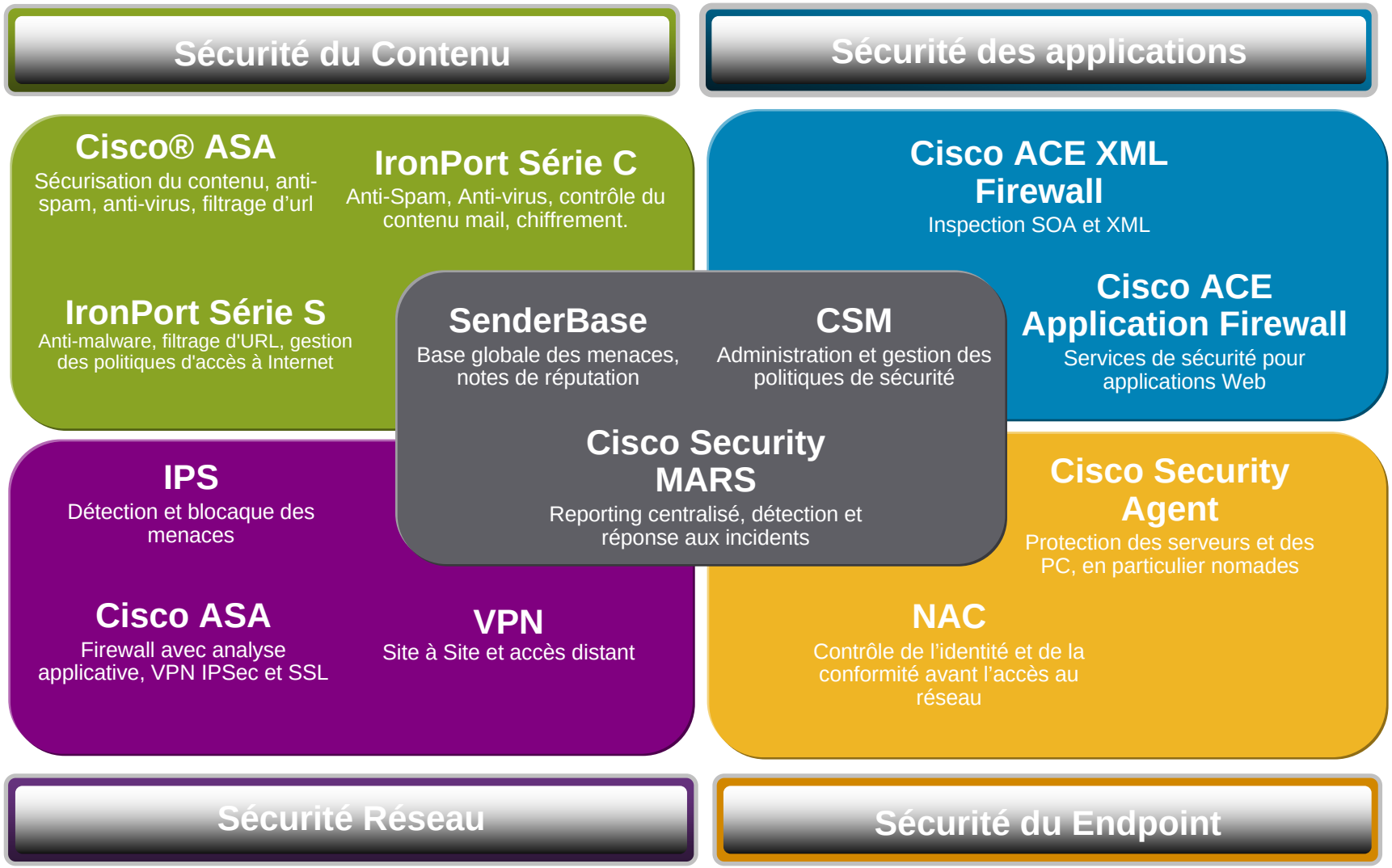
Benefices de l’approche Système



- Complex environment
- Gaps & inconsistency
- Lower visibility
- More difficult to manage

- Simplified environment
- Tighter integration = tighter security
- Greater visibility
- Easier to deploy & manage

La gamme de Solutions



Agenda

- Stratégie de sécurité Cisco
- Gamme de solutions
  - Sécurité Réseau
  - Sécurité Endpoint
  - Sécurité du Contenu
  - Sécurité des applications
  - Administration et pilotage
- Mise en application

Les solutions…
Sécurité Réseau et Endpoint

Sécurité Réseau

- Intégration de fonctions de sécurité dans l'infrastructure, virtualisation
- Services de sécurité convergent pour moins d'équipements à déployer
- Augmentation des performances pour adresser les nouveaux besoins

Principaux Produits :


Adaptive Security Appliance


Integrated Services Router

Aggregation Services Router


Cisco Switch Security Modules

Sécurité du Endpoint

- Services d'identité et de NAC
- Protection et contrôle du poste— IPS et AV

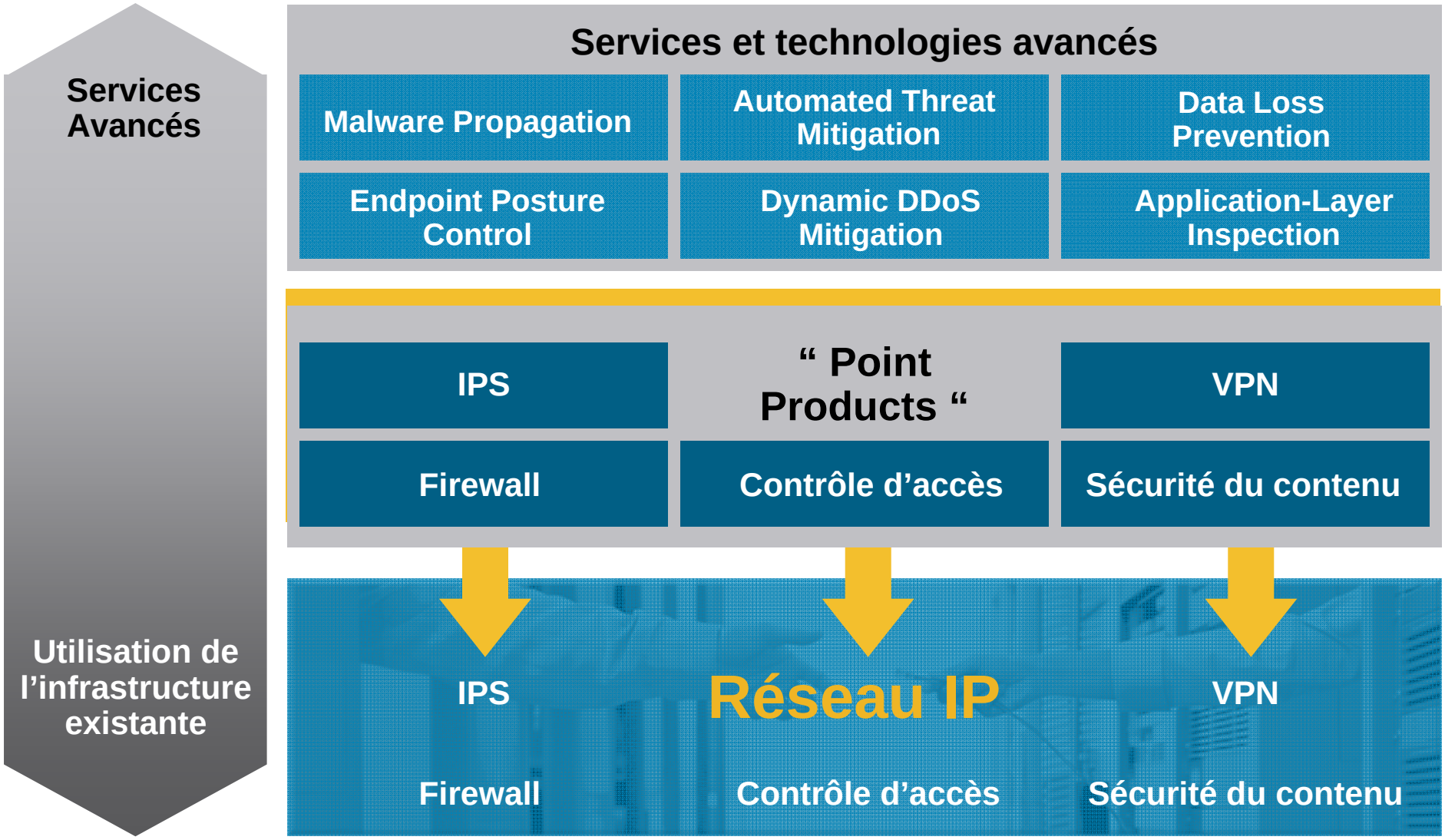
Principaux Produits :


CSA Desktop


CSA Server


NAC Appliance

La fondation du Self-Defending Network: Sécurité Réseau



Cisco ASA 5500 Series

La convergence de technologies éprouvées

Technologies Eprouvées

Technologie Firewall
Cisco PIX

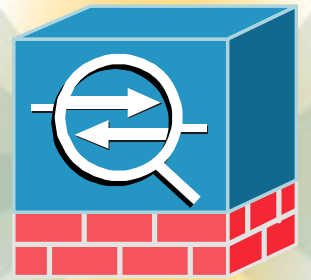
Technologie IPS
Cisco IPS

Sécurité du contenu
Trend Micro

Technologie VPN
Cisco VPN 3000

Unified Communications
Cisco Voice/Video

Intelligence réseau
Cisco Network Services



ASA 5500 Series

Protection avancée, connectivité sécurisée

Inspection Applicative, Contrôle du web, Protection de la voix/vidéo
Application Security + IPS,

Défense contre le malware et les attaques sur le contenu
Content Security Services

Contrôle du trafic
Access Control, etc.

Connectivité Sécurisés
VPN IPSec & SSL, avec fonctions évoluées

Cisco ASA 5500 Series Adaptive Security Appliances

Des solutions de la PME au Datacenter le plus performant

Cisco ASA 5500 Platforms

•L'ASA est le PIX "nouvelle génération". Il délivre les fonctions du PIX plus de nombreuses autres.

Les avantages de l'ASA par rapport au PIX

- Un meilleur rapport prix/performance
- Des options de connectivité améliorées au travers du VPN SSL
- Plus de sécurité avec l'Anti-X et l'IPS

New

ASA 5580-40

New

ASA 5580-20

ASA 5550

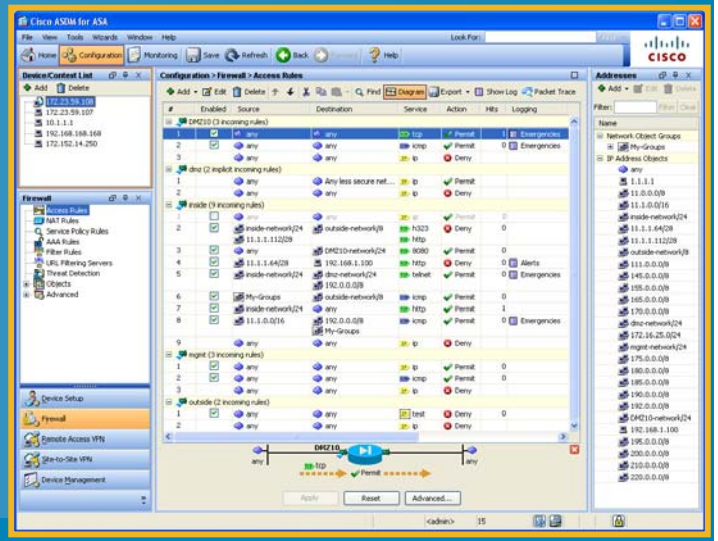
ASDM v6

ASA 5540

ASA 5520

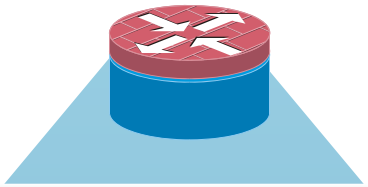
ASA 5510

ASA 5505



Teleworker | Branch Office | Internet Edge | Campus | Data Center

Cisco Integrated Services Router
Sécurité du WAN et des sites distants



Solutions de sécurité

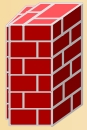

Business Continuity

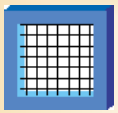
Secure Voice


Secure Mobility


Compliance

Contrôle des menaces intégré


Advanced Firewall


Content Filtering


Intrusion Prevention

Flexible Packet Matching


Network Admission Control


802.1x


Network Foundation Protection

Connectivité Sécurisée


GET VPN


DMVPN


Easy VPN


SSL VPN

Admin. et instrumentation

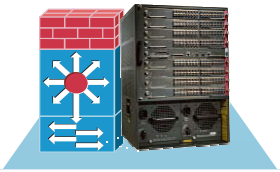

SDM


Role-Based Access


NetFlow


IP SLA

Cisco Catalyst 6500 Series
Sécurité intégrée au commutateur



Défense contre les menaces

Défendre la périphérie

Integrated FW/IPS Service Module

Protect l'interne:

Catalyst Integrated Security Toolkit

Défendre contre les attaques

Intrusion Protection System (IPS)

Protection contre les déni de service:

CoPP, CPU Rate Limiters, Netflow, QoS

Securiser les données en transit:

IPSec VPN SPA

Identité et confiance

Identity-Based Networking

Control Who/What Has Access

Enforce endpoint Security Compliance

Secure Apps.

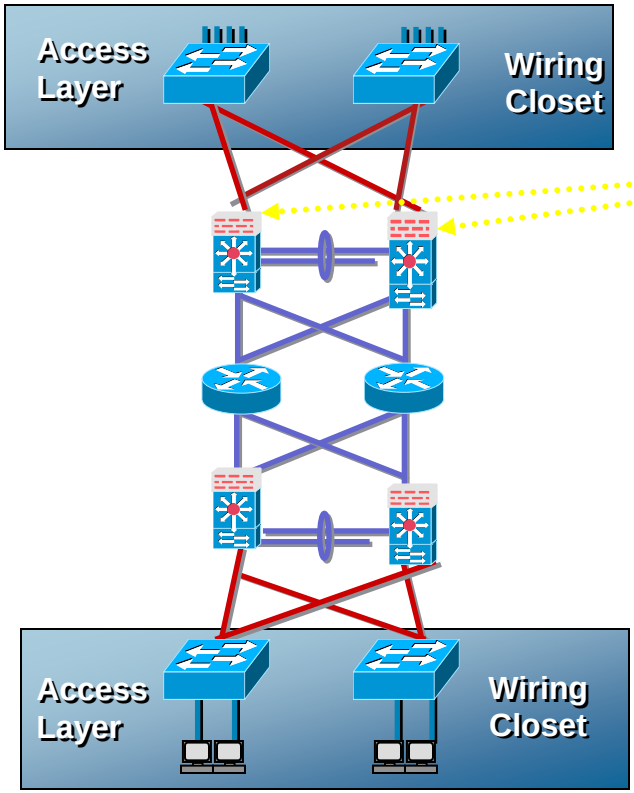
Deep Packet Inspection

Programmable Intelligent Service Accelerator (PISA)

Security and application intelligence

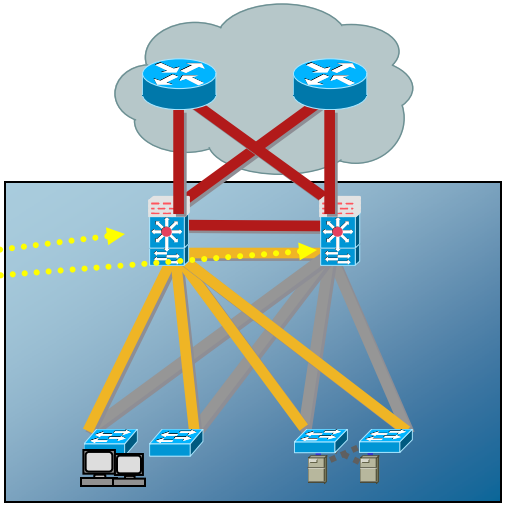
Scénarios de déploiement FWSM

Campus
Protection Interne

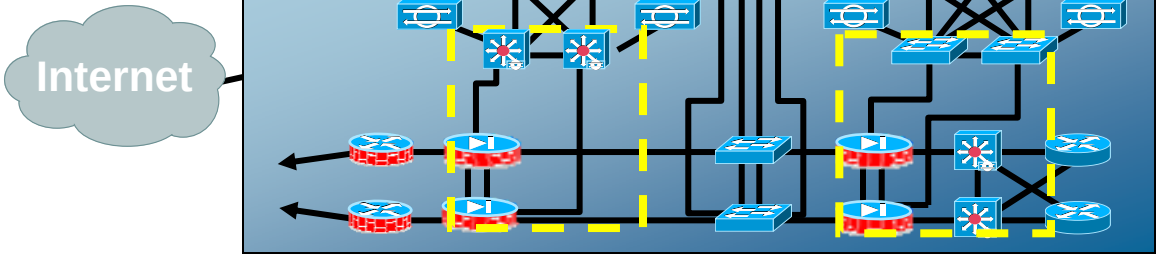


FWSM
5+ Gbps

Data Center
Filtrage du trafic malicieux



Internet DMZ & Extranet
Protection des fermes de serveurs



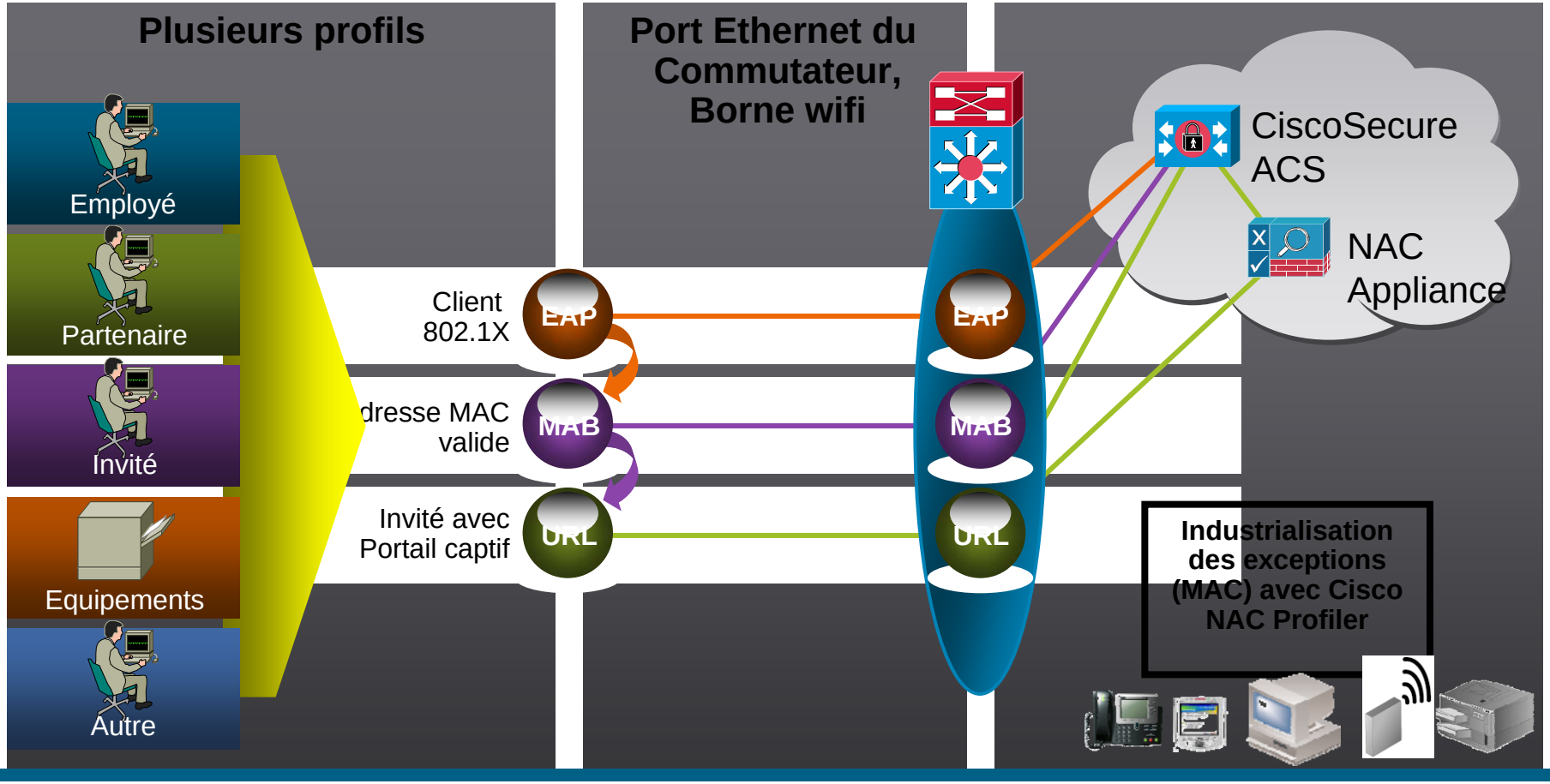
Cisco Security Agent
Protection des PC et des serveurs

- Architecture de sécurité préventive (H-IPS) sans update, avec antivirus intégré
- Un seul client, une seule interface de gestion
- Collaboration avec les équipements de sécurité réseau
- Identification et contrôle des informations importantes (DLP)

Bénéfices :

- Permet à l'IT d'adresser les risques business
- Impose les politiques de sécurité, et protège les ressources critiques
- Diminue le temps d'administration et les coûts

Identité appliquée au réseau
solutions 802.1x



Simplifier l'authentification :

Une seule méthode/configuration couvre tous les cas

Cisco Network Admission Control (NAC)

Déploiement Flexible	Services NAC innovants
Layer 2, Layer 3	Contrôle de conformité
In-band, Out-of-band	Remédiation
Centralisé, Distribué	Profiling
Module ISR	Gestion des invités
SNMP, RADIUS	

Features

- Fonction de NAC (network access control) pour renforcer la sécurité
- Gestion complète du cycle: découverte, assessment, enforcement, et remédiation
- Agent persistant et non persistant (web-based)

Bénéfices

- Securise à la fois les postes managés et non managés
-

Les solutions…
Sécurité du contenu et des applications

Sécurité du contenu

- Basé sur la réputation, protection day-0
- Capacité à adresser différents types d'attaques
- Sécurise toutes les sources de trafic

Principaux produits :

Ironport Email

Ironport Web

Intrusion Prevention Systems

Sécurité des applications

- Protection niveau 7 contre les vulnérabilités applicatives
- Inspection et validation du trafic XML
- Inspection en profondeur des paquets

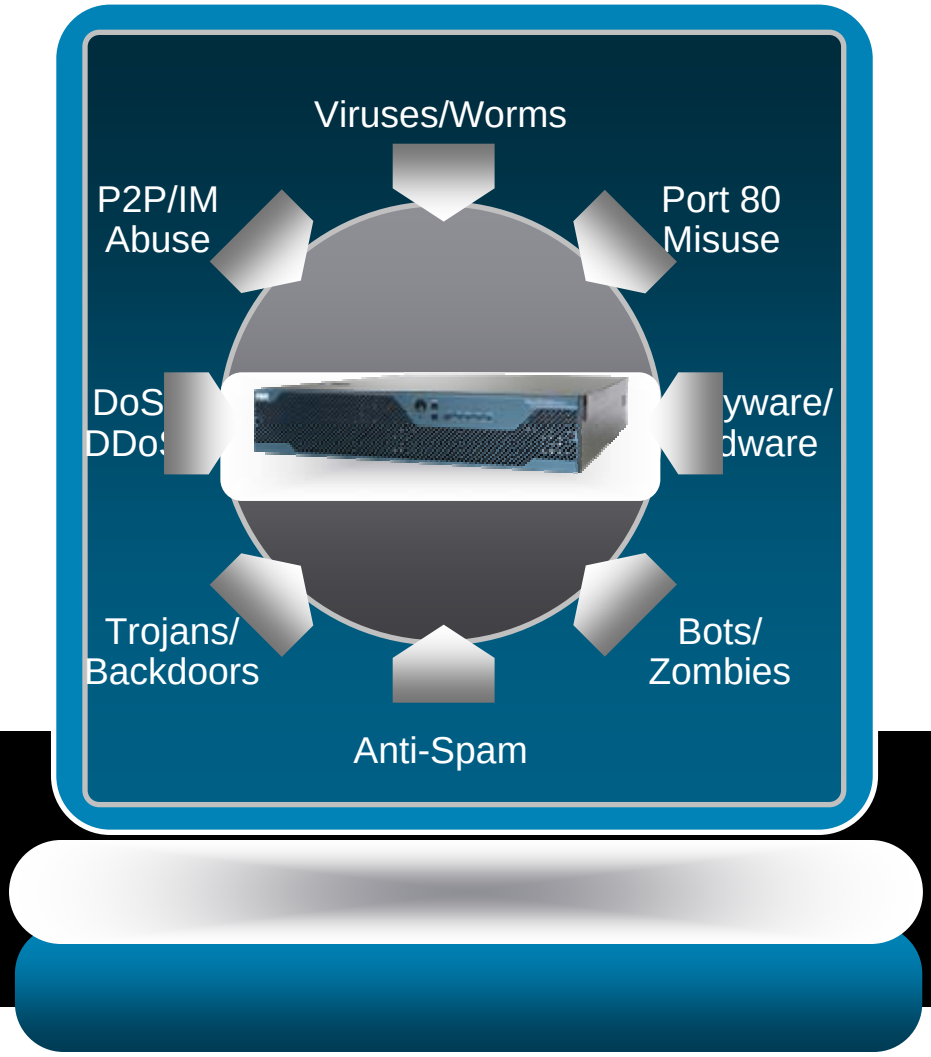
Principaux produits:

ACE XML Gateway

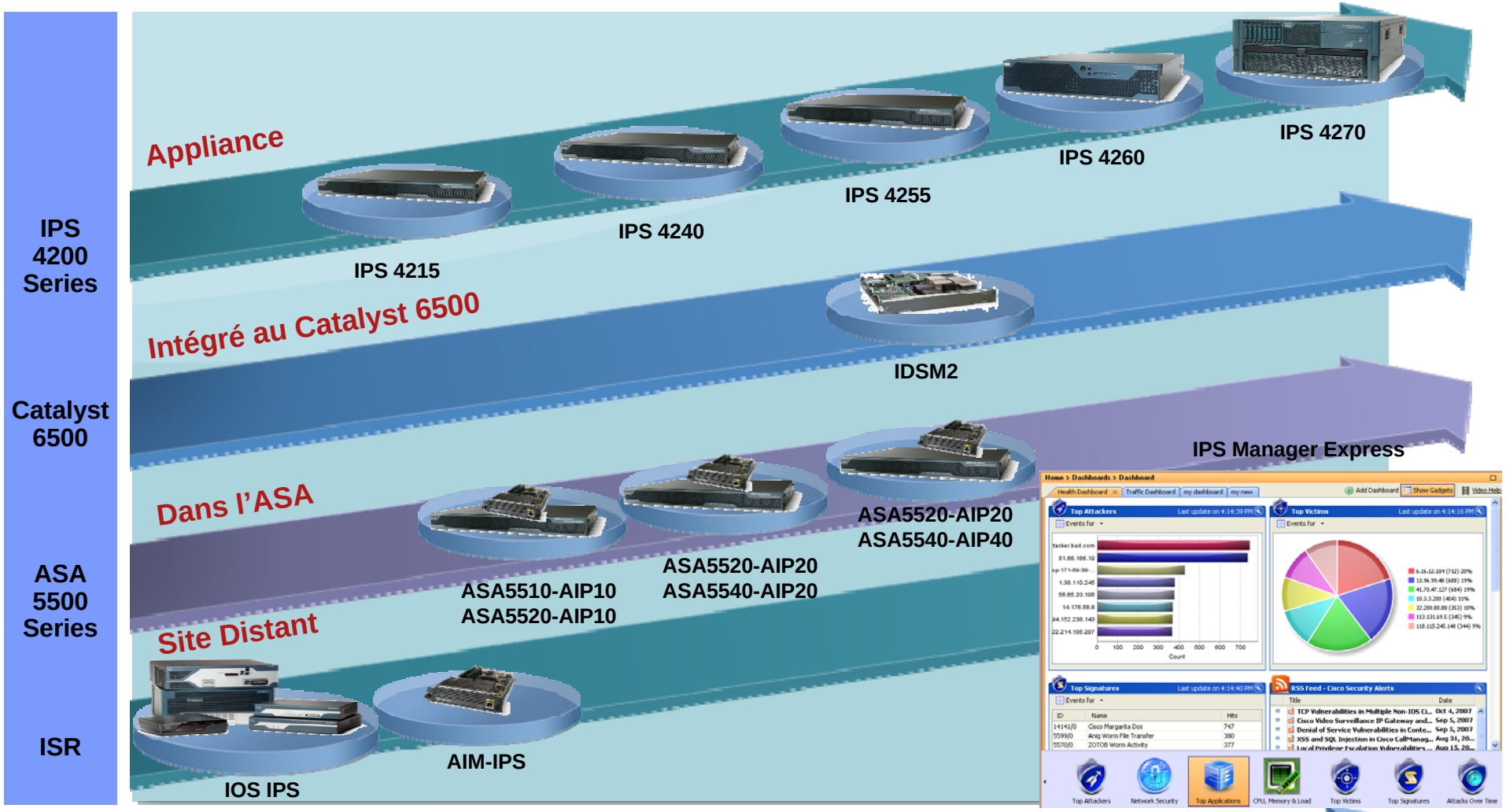
Web Application Firewall

Prévention d’intrusions réseau

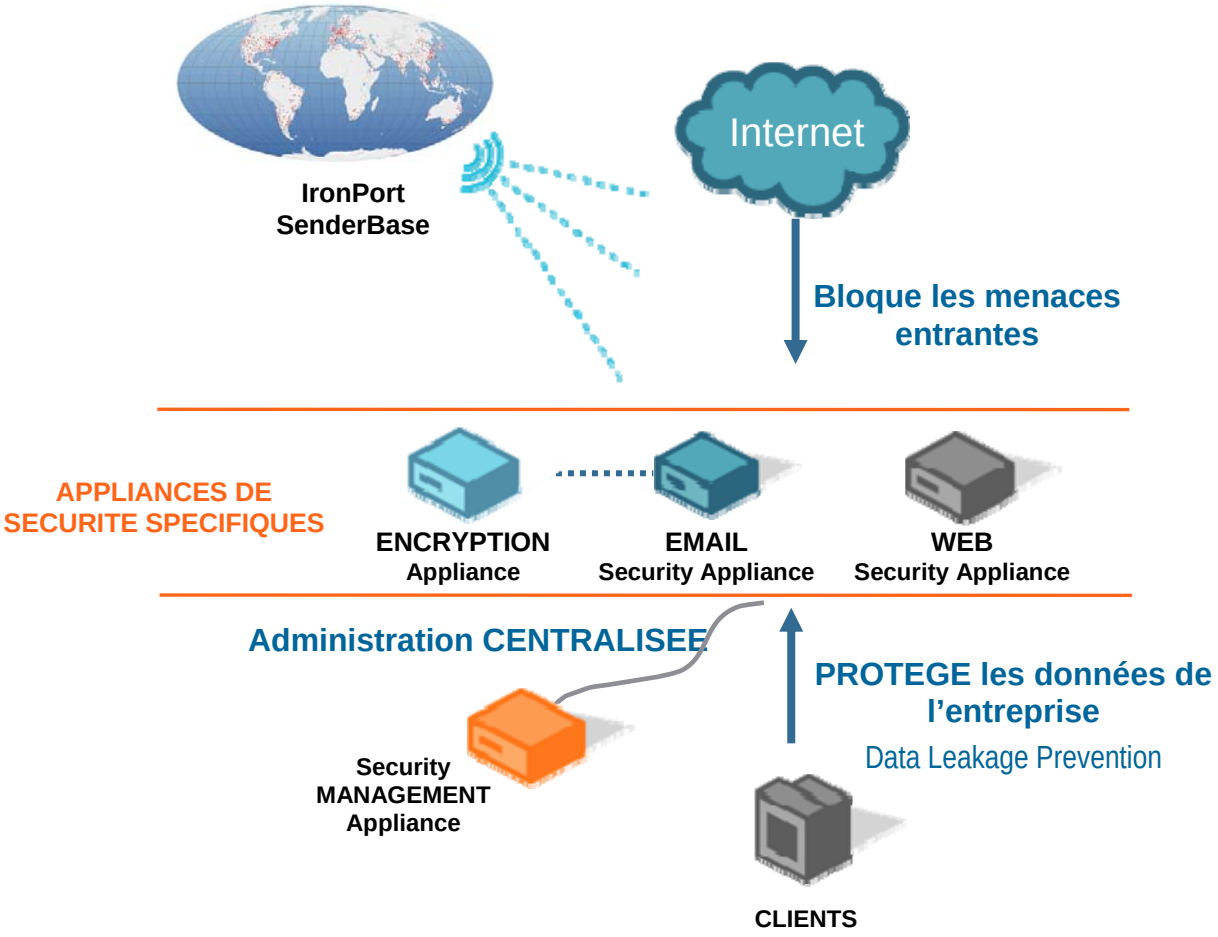
- Audit du trafic réseau, en profondeur
- Technologie de détection avancées, réduisant les faux positifs
- Coordinated response with existing network gear
- Contrôle des applications d’IM, P2P, backdoors…
- Partenariat avec TrendMicro pour les signatures “malware”



Cisco IPS – Les solutions



IronPort Gateway Security Products



Web Security | **Email Security** | **Security Management** | **Encryption**

IronPort SenderBase®

Détection des alertes et création de scores de réputation

- **Statistiques sur plus de 30%** du trafic E-Mail mondial
- Détection des nouvelles alertes
- Plus de **150 paramètres E-Mail & Web** pris en compte pour établir les scores de réputation

- *Volume de données*
- *Composition du message*
- *Plaintes*
- *Blacklists, whitelists*
- *Données hors-ligne*

E-Mail Reputation Filters → **Score de réputation**

- *blacklists et whitelists d'URL*
- *Contenu HTML*
- *Infos sur le domaine*
- *URL à problèmes "connues"*
- *Histoire du site Web…*

Web Reputation Filters → **Score de réputation**

Introducing Cisco ACE Web Application Firewall

- **Nombreuses signatures d'attaques HTTP/XML telles que : SQL Injection, buffer overflow, cross-site scripting, cooking/session poisoning, etc.**
- **Permet de satisfaire la norme PCI Section 6.5 et 6.6**

Web Application Firewall

•Protège les applications métier HTTP et HTML des attaques

Protection contre les menaces sur les architectures SOA, Web Services, et XML

•Secures and offloads web services transactions

Protection Complète Applicative des flux HTTP et XML

Les solutions…
Administration et pilotage de la sécurité

Gestion de la sécurité

- Gestion opérationnelle efficace tout en minimisant les ressources
- Gestion du cycle de vie des incidents de sécurité en environnement multi-vendeur
- Tableau de bord
- Interaction entre le monitoring et la configuration
- Utilise les informations d'identité pour les appliquer au réseau (ACS)

Principaux produits


Cisco Security MARS

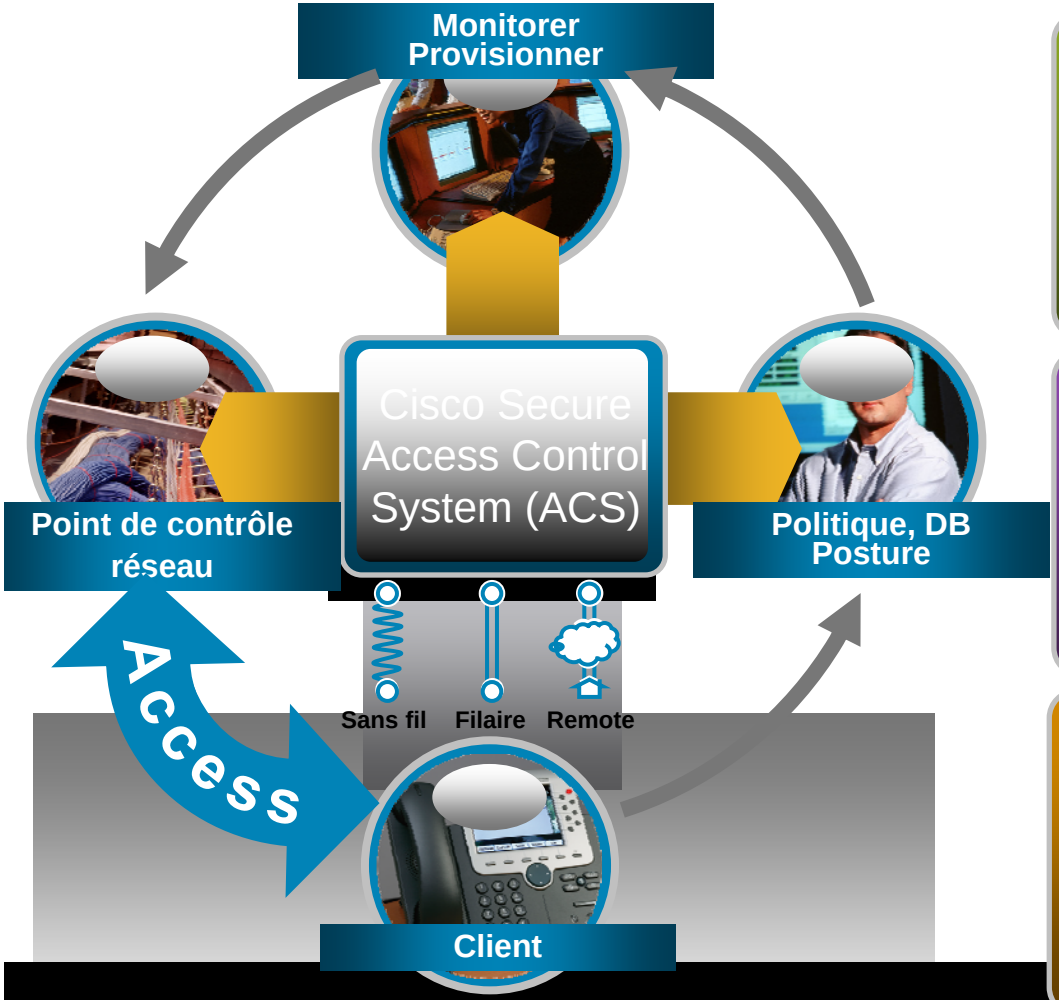

Cisco Security Manager


CiscoSecure ACS


TrustSec

Cisco Secure ACS

Au coeur de la stratégie d'identité



Pivotal
Element clé de la stratégie ID et accès

- Support de multiples bases de données
- Posture, audit et conformité

Puissant
Plateforme d'accès robuste

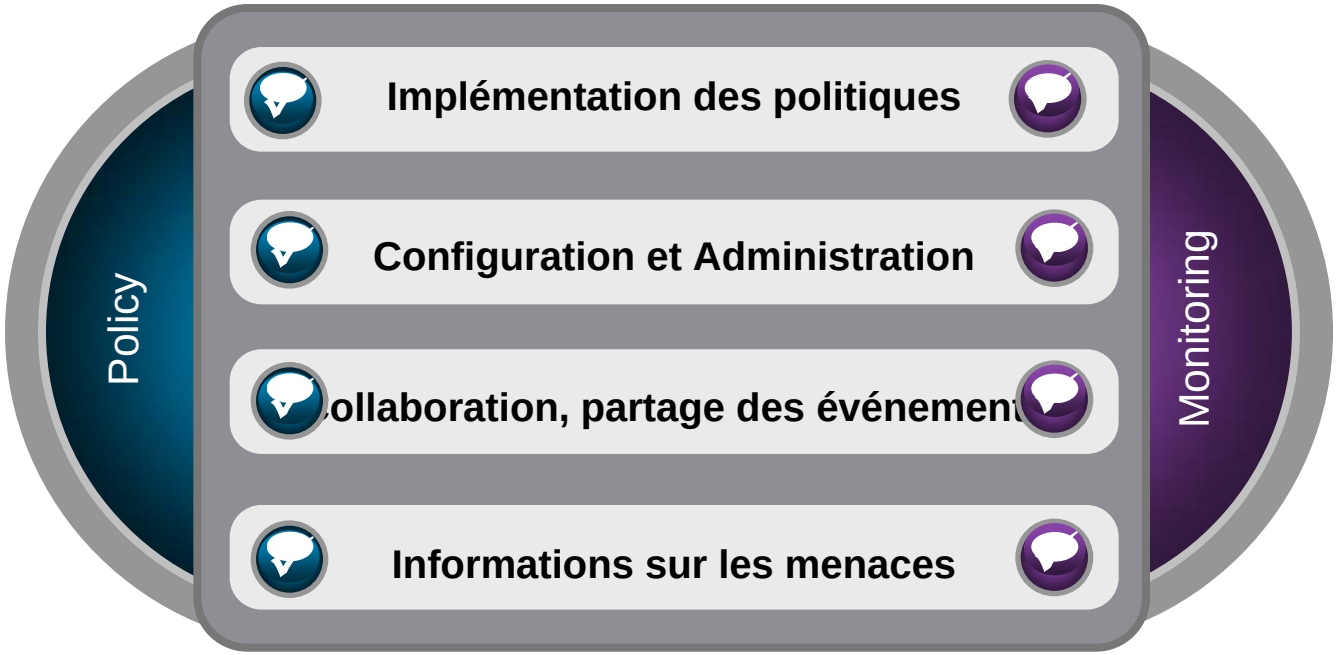
- Performance évolutive
- Appliance ou logiciel, ACS Express pour SMB

Trusted
The World's #1 ID and Access System

- Plus de 100,000 unités vendues
- 94% de taux de satisfaction*

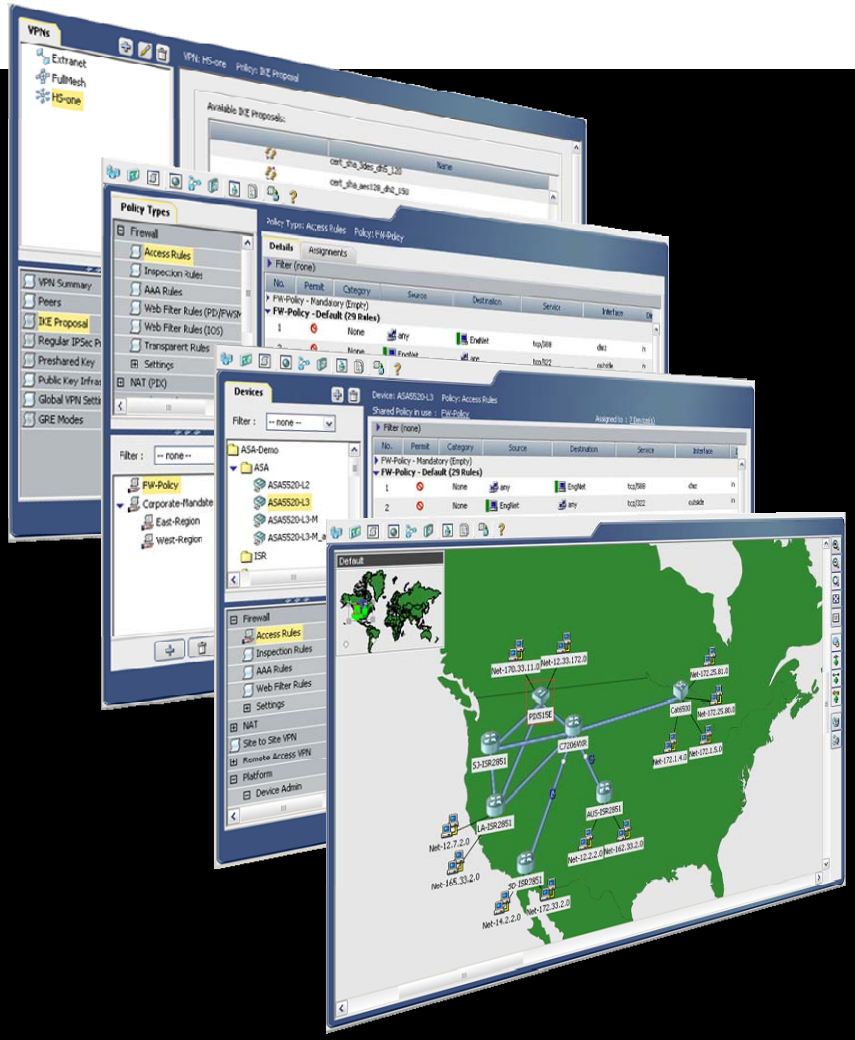
**Results of customer survey January 2008*

Une gestion complète



Moins de complexité pour plus d’efficacité

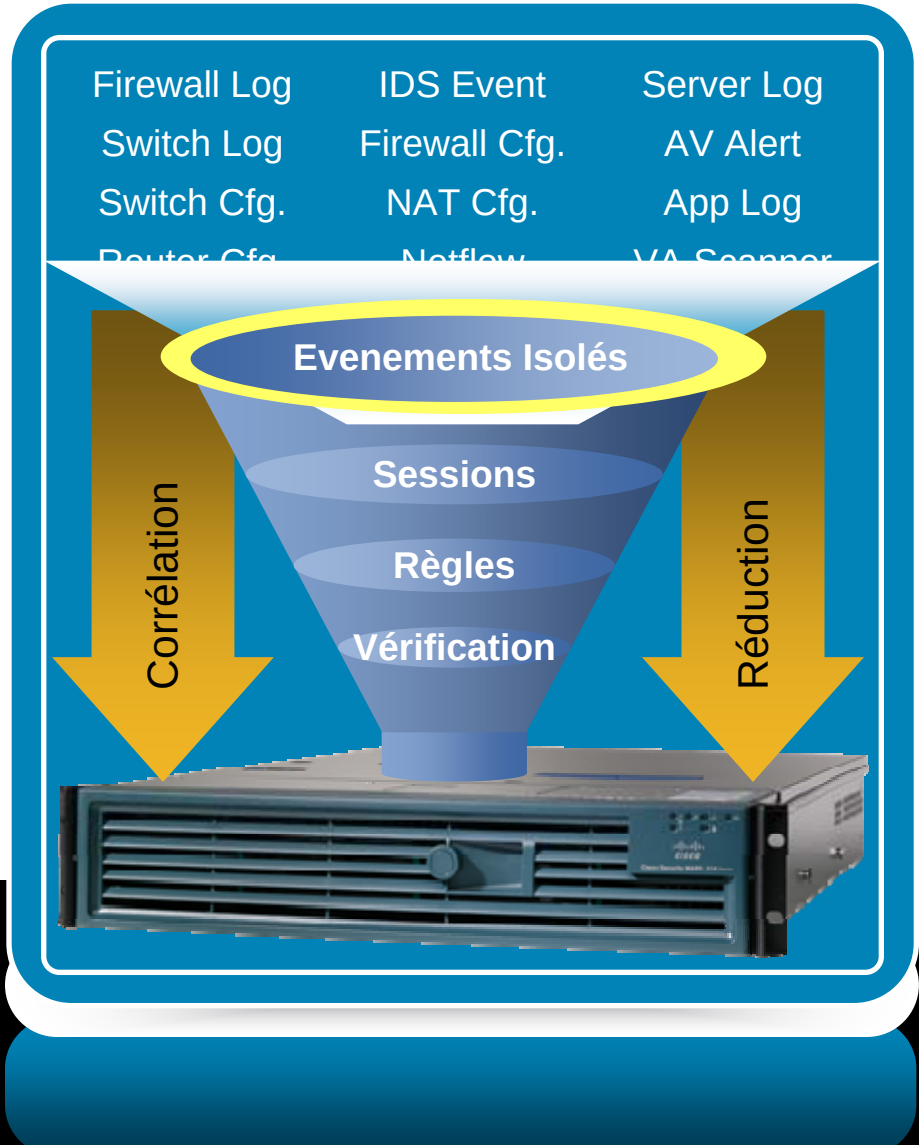
Cisco Security Manager



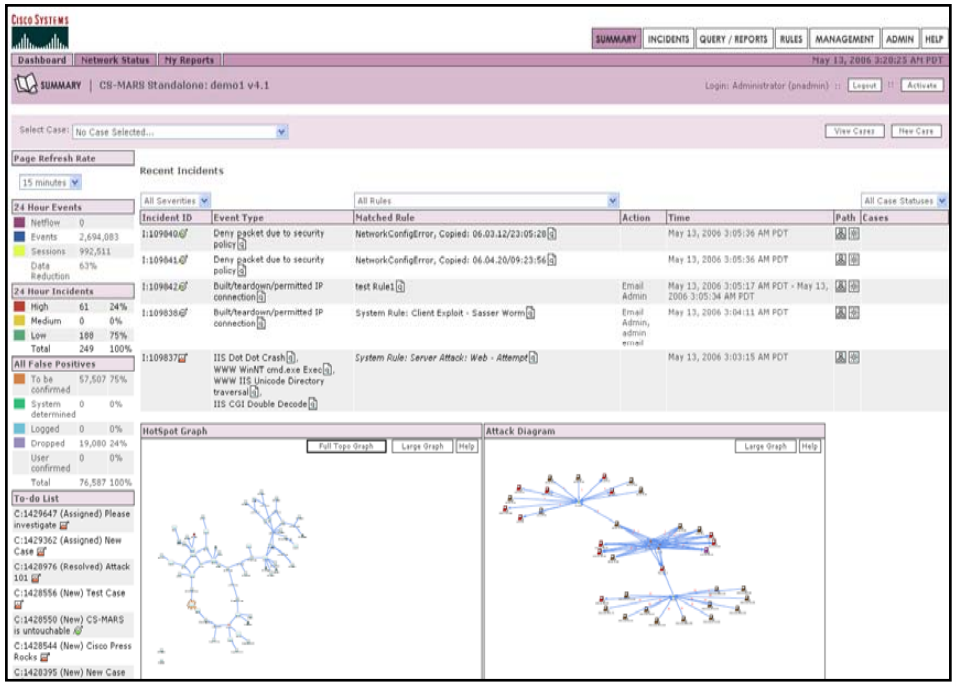
- Permet la gestion de la

Cisco Security MARS

- Appliance de gestion des incidents de sécurité
- Détection et isolation rapide des menaces
- “Centre de commandement”
- Corrèle les informations provenant des équipements de sécurité et du réseau, dans un environnement multi-vendeurs

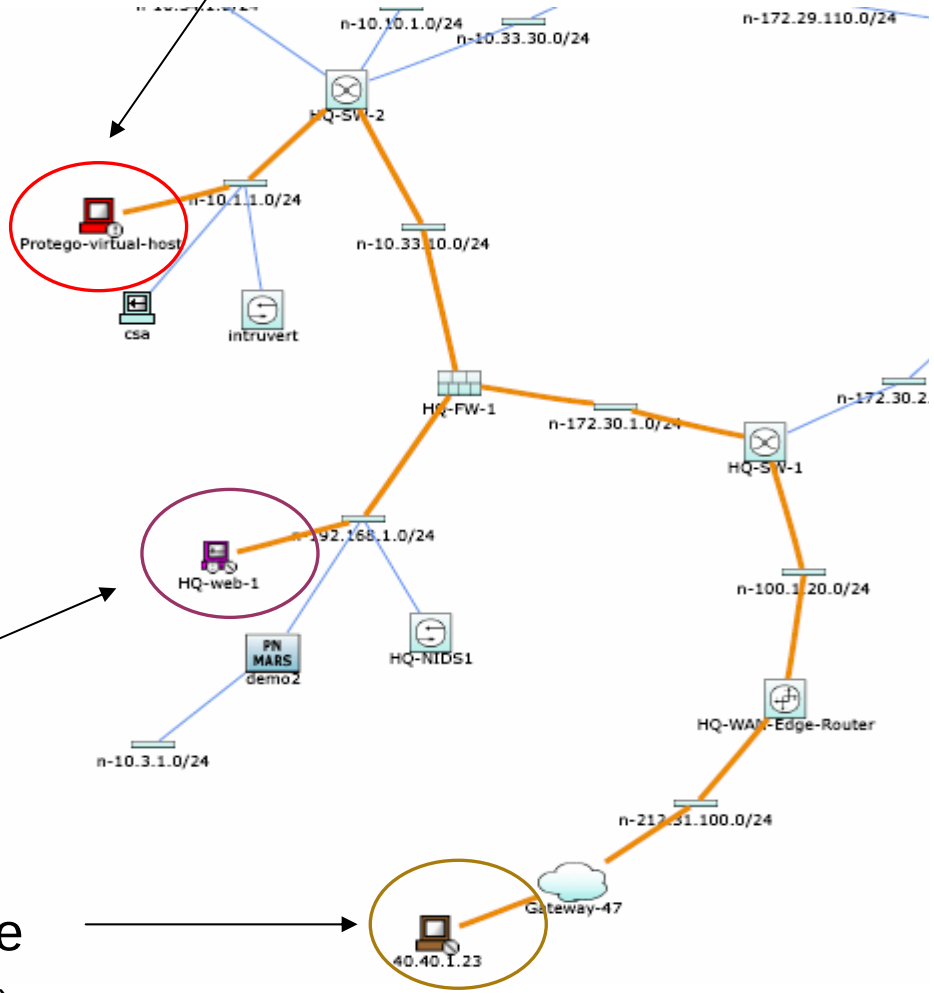


Cisco MARS en action



Victime

(rouge)



Machine compromise, source de rebond

(violet)

Source

(marron)

Agenda

- Stratégie de sécurité Cisco
- Gamme de solutions
- Mise en application :
  - –Protection contre la propagation du malware
  - – Prévention de la fuite d’information (DLP)
  - – Contrôle d’accès et identité

Une approche système pour se protéger du malware: Visibilité et Contrôle

Firewall et VPN

- Contrôle d'accès du trafic
- Chiffrement

Prévention D'intrusion

- Détection
- Réponse ciblée

Sécurité du Contenu

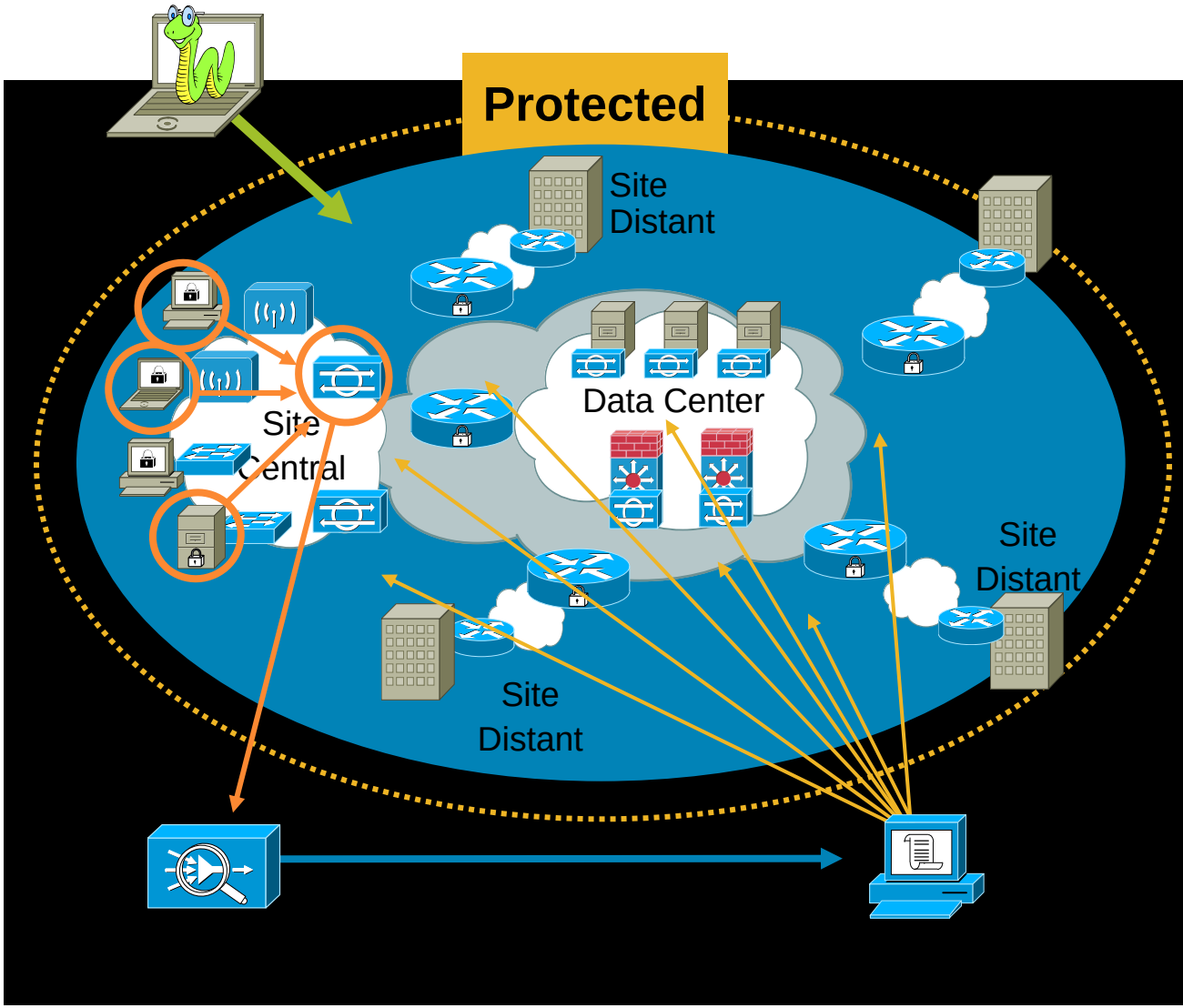
- SPAM Email
- Filtrage Web

Sécurité du Endpoint

- Host IPS
- Solution anti-virus

Gestion et monitoring centralisé

Une solution intégrée pour bloquer le malware: IPS, CSA, MARS, and CSM



- Un malware tente de

Data Loss Prevention (DLP)
Au delà des mesures traditionnelles

- DLP: Mesures de sécurité permettant de protéger les données sensibles de l'entreprise, qu'elles soient en cours d'utilisation, en cours de transport, ou stockées
- Perte de donnée au travers des ports autorisés (web/mail)
- Perte/Vol de ressources
  - PC Portables
  - Autres équipements nomades
  - Ressources dans le datacenter

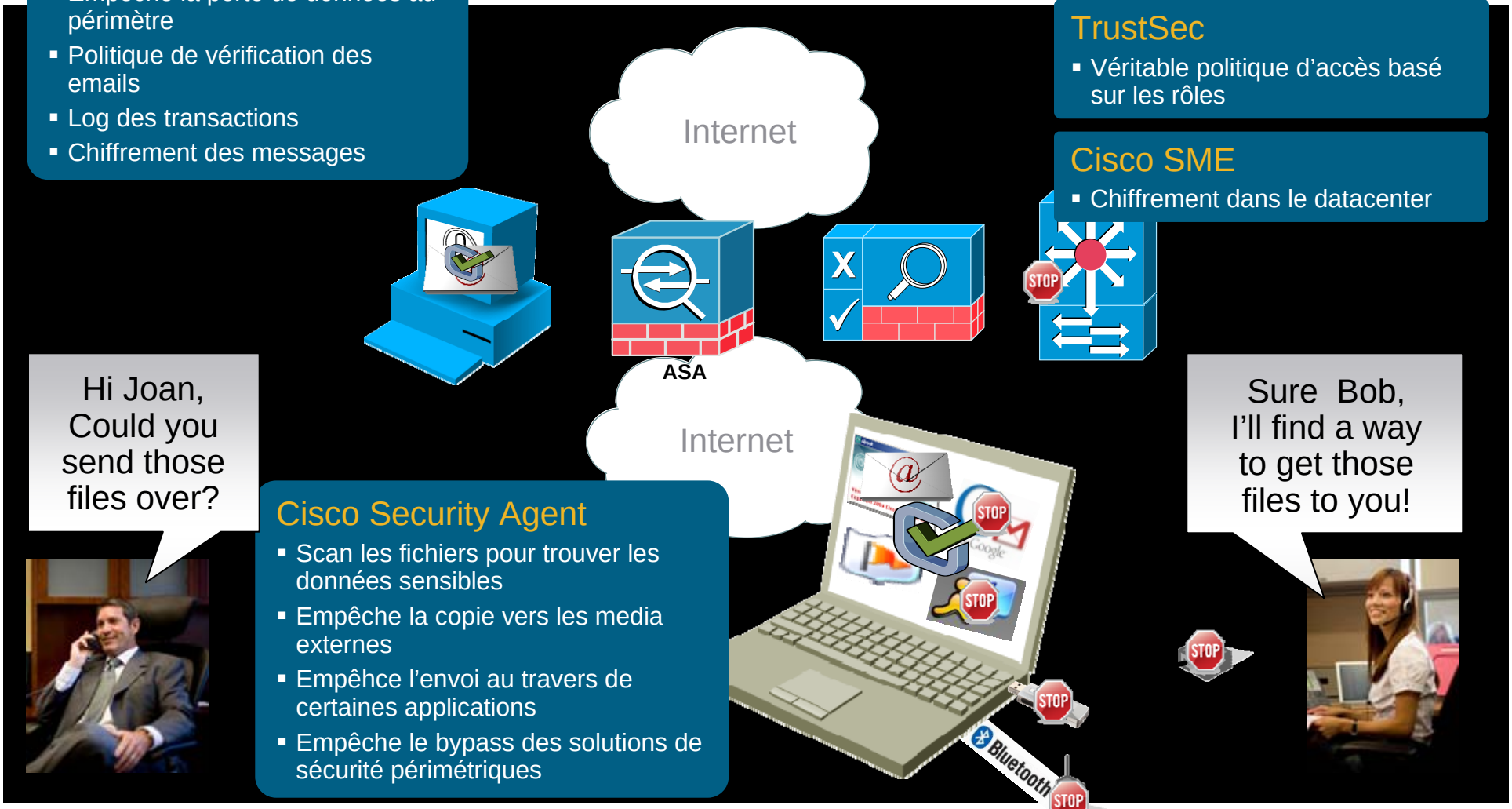
Cisco Data Loss Prevention Solution
NAC, CSA, IronPort, et TrustSec

IronPort
- Empêche la perte de données au périmètre
- Politique de vérification des emails
- Log des transactions
- Chiffrement des messages

NAC Appliance
- Vérifie que CSA est bien présent, et que la posture est saine

TrustSec
- Véritable politique d'accès basé sur les rôles

Cisco SME
- Chiffrement dans le datacenter



Cisco Security Agent
- Scan les fichiers pour trouver les données sensibles
- Empêche la copie vers les media externes
- Empêhce l'envoi au travers de certaines applications
- Empêche le bypass des solutions de sécurité périmétriques

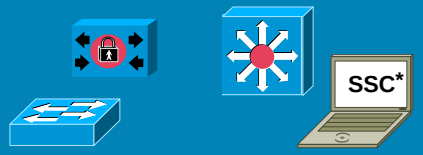
Le besoin de lier identité et réseau

- Explosion des méthodes d'accès et des profils sur les réseaux (invités, partenaires, employés…)
- Besoin de construction de bulles de sécurité, isolées, avec fonctions de filtrage avancé (firewall, IPS) entre les bulles.
- Objectif : Un service "mobile"
  - Gestion simple des politiques, par groupe d'utilisateurs et de ressources
  - Accès basé sur l'identité et la conformité
  - Déploiement simple de services et ressources, indépendemment de la géographie et de la méthode d'accès

Identity + NAC + TrustSec
Pre and Post Admission Network Services

Infrastructure Identité

- Authentification utilisateur et équipement
- Contrôle d'accès réseau
- Mobilité de l'équipement
- 802.1X/CiscoSecure ACS



* Cisco Secure Services Client

+

Services de Profiling

- profiling des devices
- Monitoring comportemental
- Reporting des devices présents

Services Invités

- Portail Guest et Sponsor
- Basé sur rôles
- Provisioning et reporting

Service de conformité

- Conformité des équipements managés et non managés
- Remédiation

+

futur

"Role-Based Access Control"

- Indépendant de la topologie
- Evolutif, via tagging

Intégrité et Confidentialité

- Protection hop-by-hop
- Préserve les services L4–L7

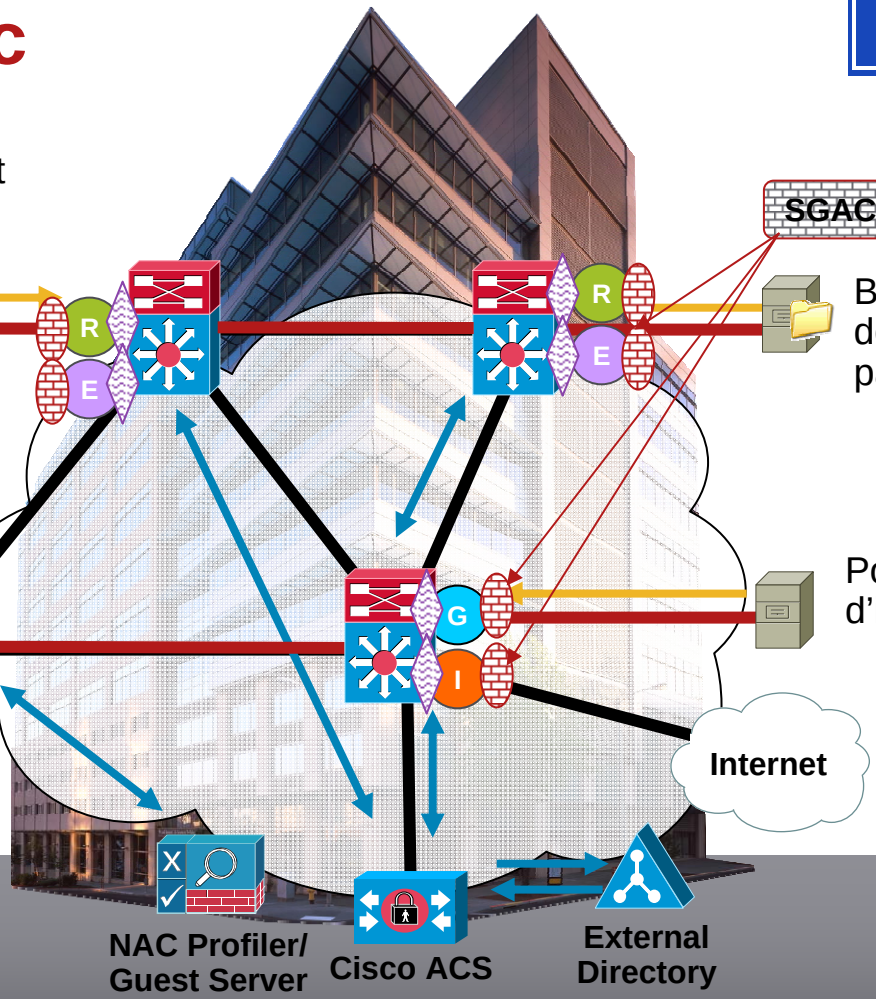
Contrôle d'admission des équip. réseau

- Authentification des équipements réseau (commutateurs, routeurs..)
- Infrastructure de confiance

Une application de l'identité
NAC, ACS, TrustSec

Les médecins mettent à jour un dossier patient

La famille a des informations temps réel



Actions	Groupes de sécurité
Ingress Tagging	E Medical Equipment
Egress Filtering	R Medical Group
	G Guest Group
	I Internet Group

Conclusion

- Self-Defending Network: des produits best of breed, dans une approche système
- Solutions de sécurité pour protéger, optimiser votre métier
- Réduction du risque; réduction de la complexité ; réduction de TCO
- L'intégration unique de la sécurité réseau et de la sécurité du contenu

cisco.fr/go/securite

Q & A