

HOW SECURE NETWORKS ARE MANAGED

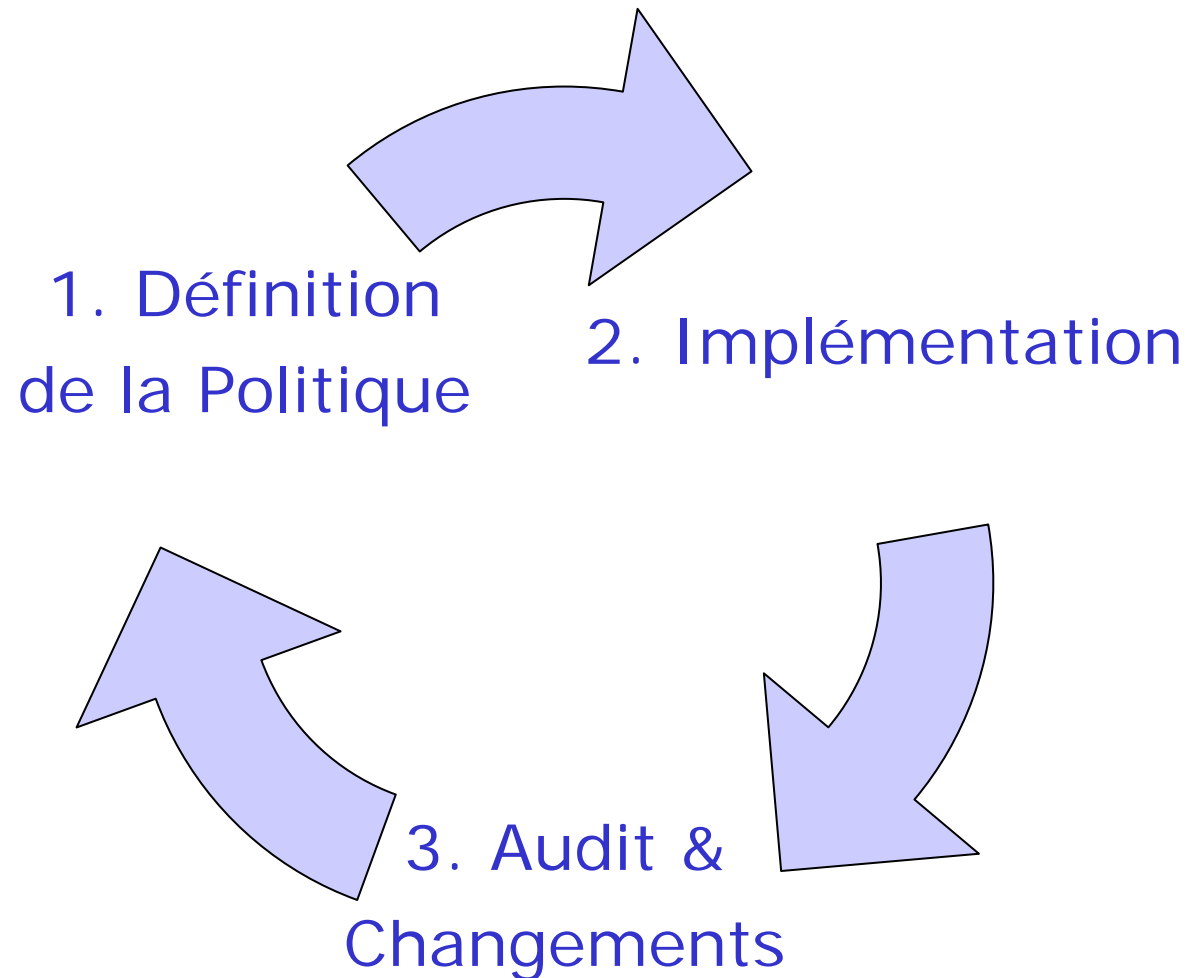
GESTION GLOBALE DES POLITIQUES DE SECURITE RESEAU



Philippe Langlois

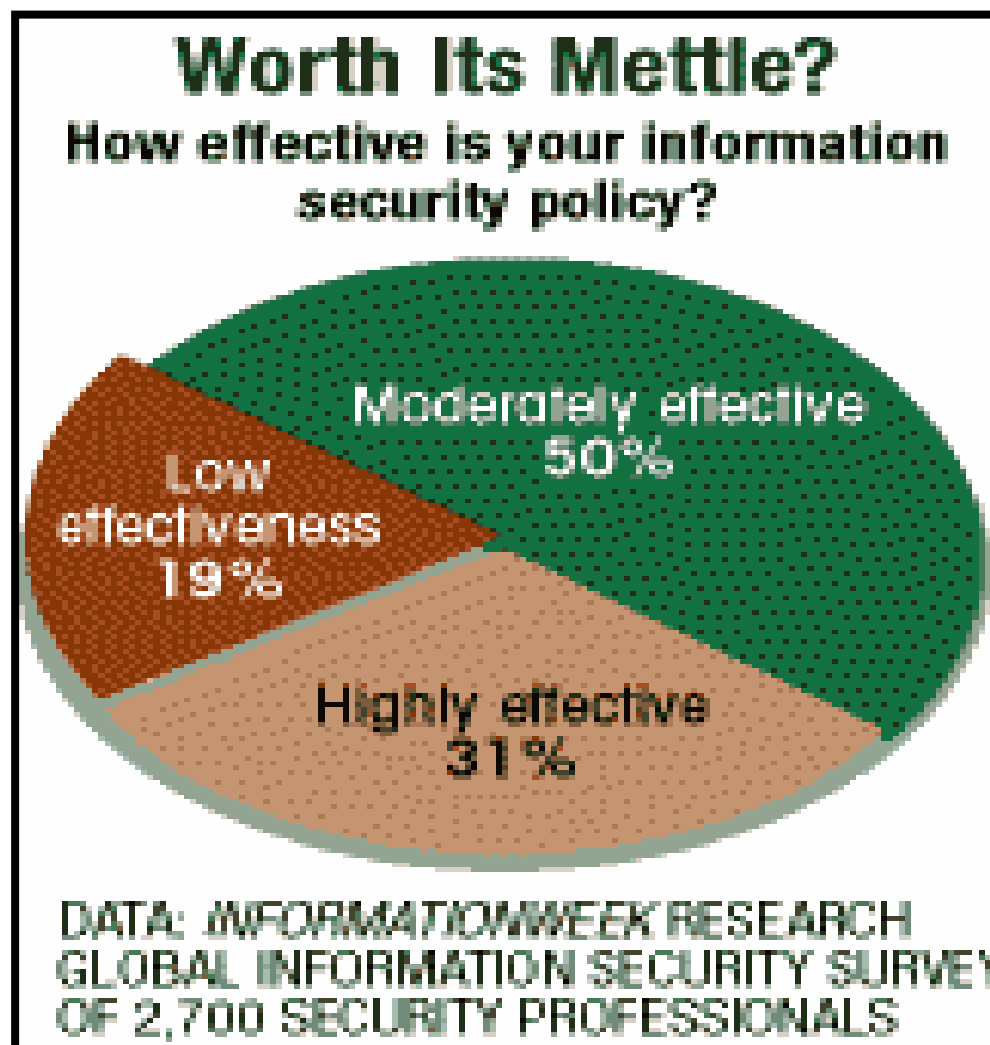
Architecte Sécurité

- **“A succinct statement of a system’s protection strategy”**
- **Adaptée aux entreprises**
 - Adaptée au business
 - Adaptée à l’architecture réseau existante
 - Adaptée aux personnes
- **Gérable**
 - Facile à déployer
 - Facile à maintenir et à adapter aux changements
 - Facile à valider
- **Communicable**
 - La politique est une vue de haut niveau qu’il faut traduire
 - Une information qui ne circule pas dans de bonnes conditions est dommageable
 - L’éducation des personnels compte autant que les règles de filtrages

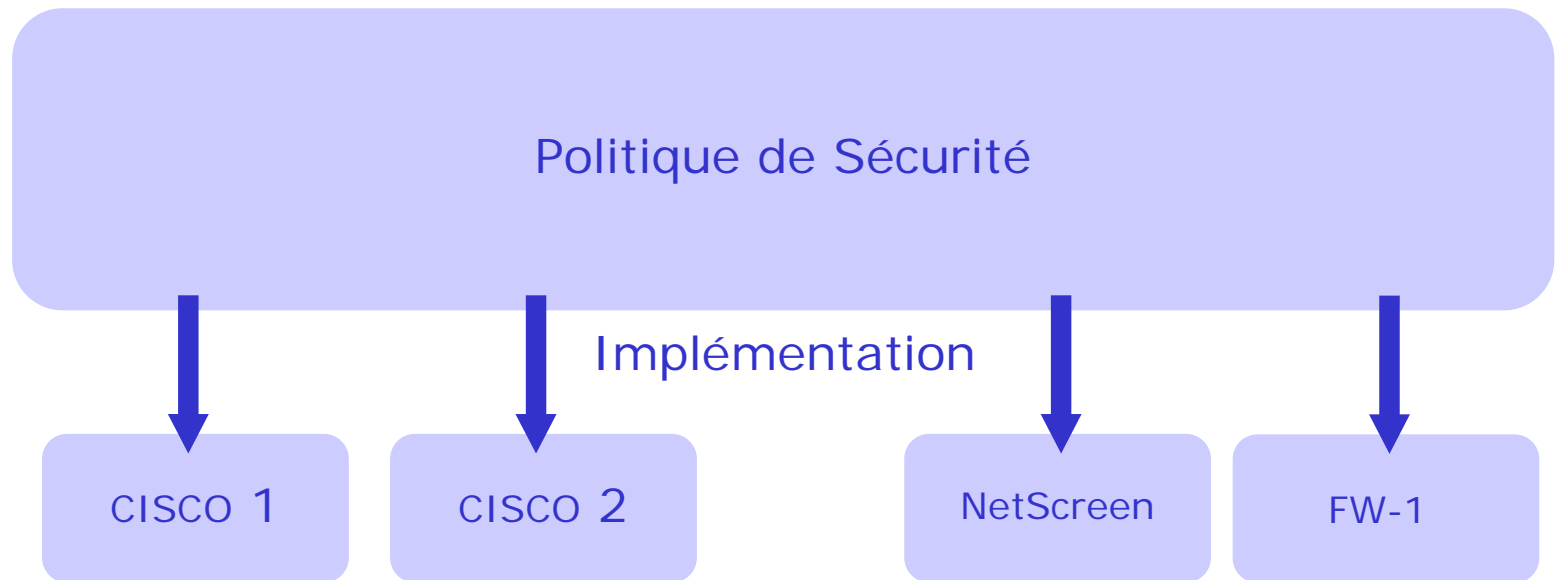
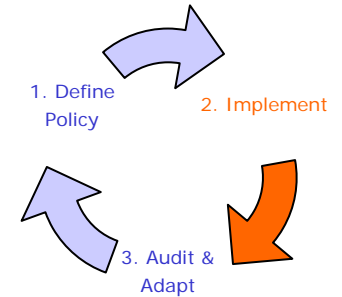


1. Définition d'une politique : Besoins du système d'information

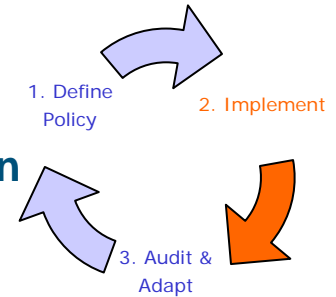
- **Questions clé**
 - Quelles informations sont critiques pour les besoins opérationnels de l'entreprise ?
 - Classification du niveau de criticité des informations, des systèmes et des réseaux ?
 - Qui a accès à quelles ressources ?
 - Quelles autorisations sont nécessaires ?
 - Quel type d'accès distants ? Accès distant vers quoi ?
 - Comment et où les informations sont-elles transmises et stockés ?
 - Comment auditer ces accès ?
 - Que faut-il faire en cas de non respect des règles définies ? Fraudes? Attaques ?
 - Qui est responsable ? Comment communiquer sur les problèmes ?
- **Basé sur le "CISSP Certification Exam Guide", S. Harris.**



- **Convertir le modèle de haut niveau (politique de sécurité)**
- **Le découper suivant les périmètres**
- **Prendre en compte les spécifications de chaque équipement**

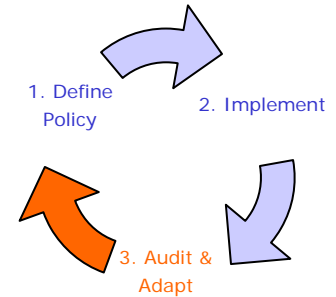


- **Multitudes de langages et d'interfaces différentes**
- **Difficile d'avoir une vue globale après implémentation**
- **Les process manuels sont coûteux**
 - Le temps dédié à l'administration ne diminue jamais
 - Différents types d'équipements : X jours de formation, configuration initiale
 - Nombre d'équipements : X jours par configuration d'équipement
- **Les interactions sont un cauchemar**
 - NATs
 - VPNs & tunnels
 - La complexité est un facteur de ralentissement même s'il existe des procédures
- **Conséquences : Diminution de l'hétérogénéité des équipements**
 - Va à l'encontre des recommandations des experts
 - Limite l'accès à de nouvelles fonctionnalités, a un impact sur le budget, diminue la capacité de changements rapides

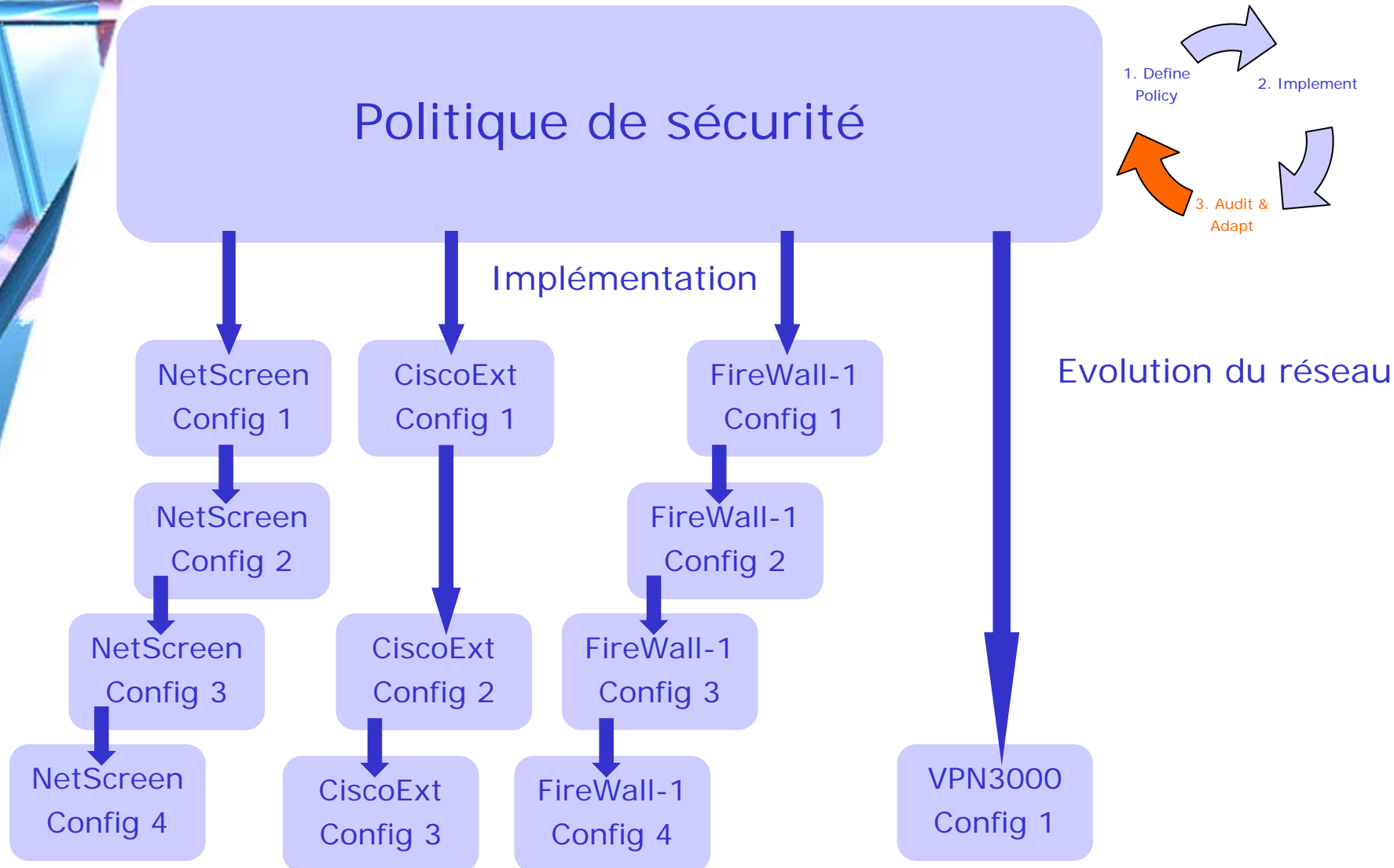


3. Adapter et Auditer : Problème de flexibilité

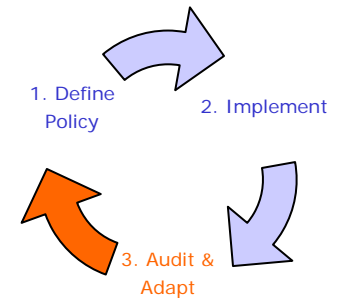
- **Puisque les configurations manuelles sont difficiles**
 - Vous minimisez les points de filtrages
 - Vous n'utilisez pas tout le potentiel de vos équipements
- **Disponibilité des administrateurs**
 - Vous dépendez fortement de la disponibilité de vos administrateurs de firewalls
- **Si vous êtes sage, vous construisez une politique de filtrage fine**
 - Ce qui induit des configurations redondantes ce qui complexifie l'administration
- **Si vous faites une modification temporaire**
 - Elle a de fortes chances de perdurer car on ne touche pas à quelque chose qui fonctionne !



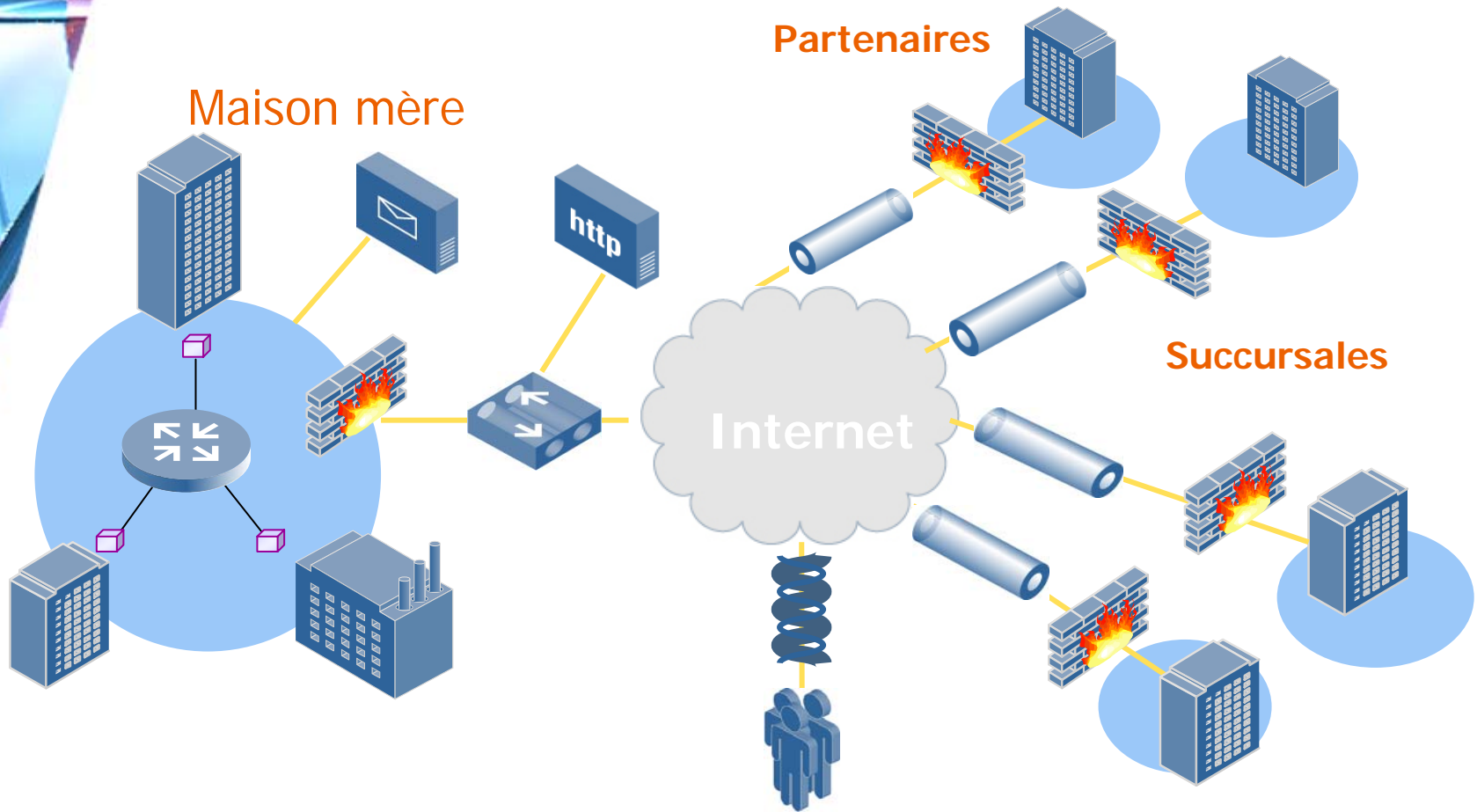
3. Adapter et Auditer : Maîtriser la divergence pendant l'évolution



- **Les configurations divergent du modèle originel**
 - Besoins business
 - Évolution dans le temps
 - Difficile de suivre qui a fait quoi, comment et pourquoi
- **Le problème s'accroît avec l'évolution de la taille du réseau**
 - La taille double, la complexité quadruple
 - La communication devient de plus en plus difficile à gérer
- **Problématique des sites distants**
 - Définition de politiques communes avec des besoins différents
 - Équipes différentes qui s'impactent à chaque changement



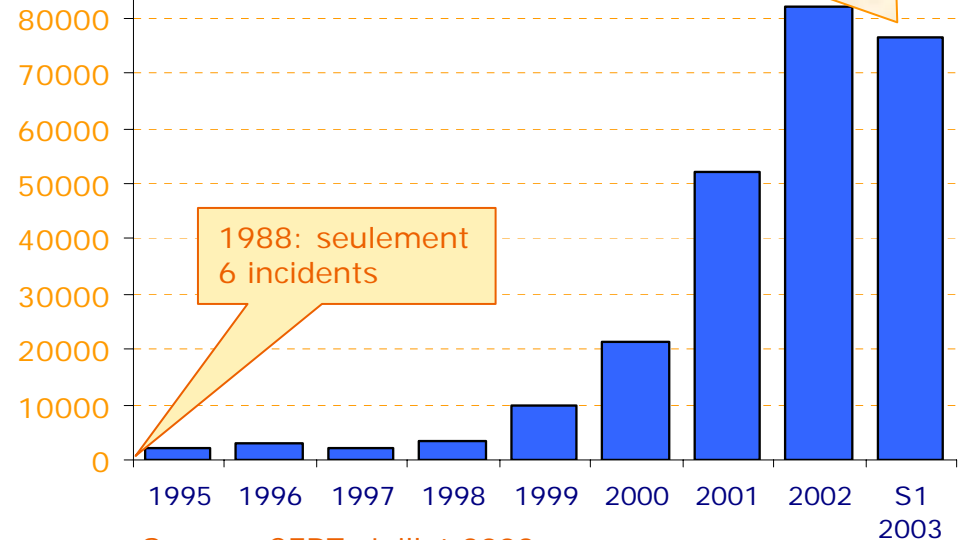
Complexité croissante du réseau



- En 2003, les budgets sécurité IT représenteront plus de 10% du total IT aux USA (CSO magazine)
- Moyennes des pertes lorsque l'incident a un impact : 1.8 M\$ (CSI/FBI)
- 90% des grandes sociétés américaines ont eu des incidents en 2001-2002

Incidents de sécurité déclarés au CERT

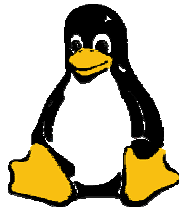
d'incidents



Source: CERT, Juillet 2003

- **Produire une solution de gestion robuste et évolutive pour les entreprises et administrations qui souhaitent un contrôle total de leur sécurité réseau**
- **Les produits Solsoft :**
 - Permettent de mettre en place des politiques de sécurité de manière collaborative et efficace
 - Fiabilisent la gestion de la sécurité réseau
 - Baissent le coût de gestion en environnement multi-constructeur
- **Le but:**
 - Éliminer le risque sécurité réseau

- **Éditeur de logiciel français**
 - Couvertures commerciales principales : USA (2/3), UK, Allemagne et France (1/3)
 - R&D en France
- **Plus grande levée de fonds Européennes dans les logiciels en 2003**
 - 10€ millions
 - The Carlyle Group (US)
 - Credit Lyonnais Asset Management (France)
 - Rotschild (France)
 - Logispring (Suisse)
 - Un total de 32€ millions de capitaux
- **Une équipe de management dont les membres sont issus de :**
 - Qualys, Microsoft, Oracle, Cisco, Check Point, Symantec, Network Associates, BMC, ISS,...



Points d'application de la sécurité

Firewalls



Boîtiers VPN

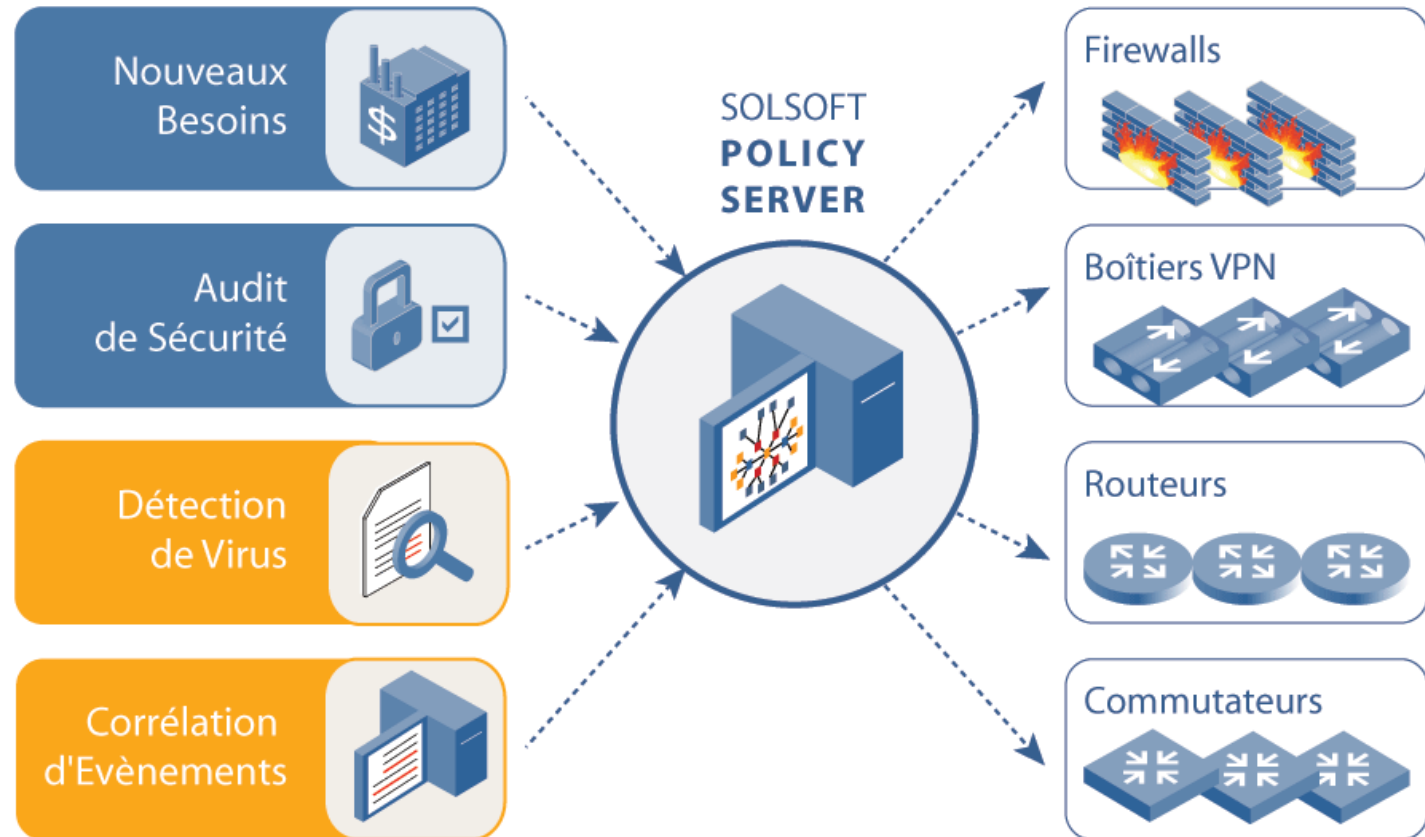


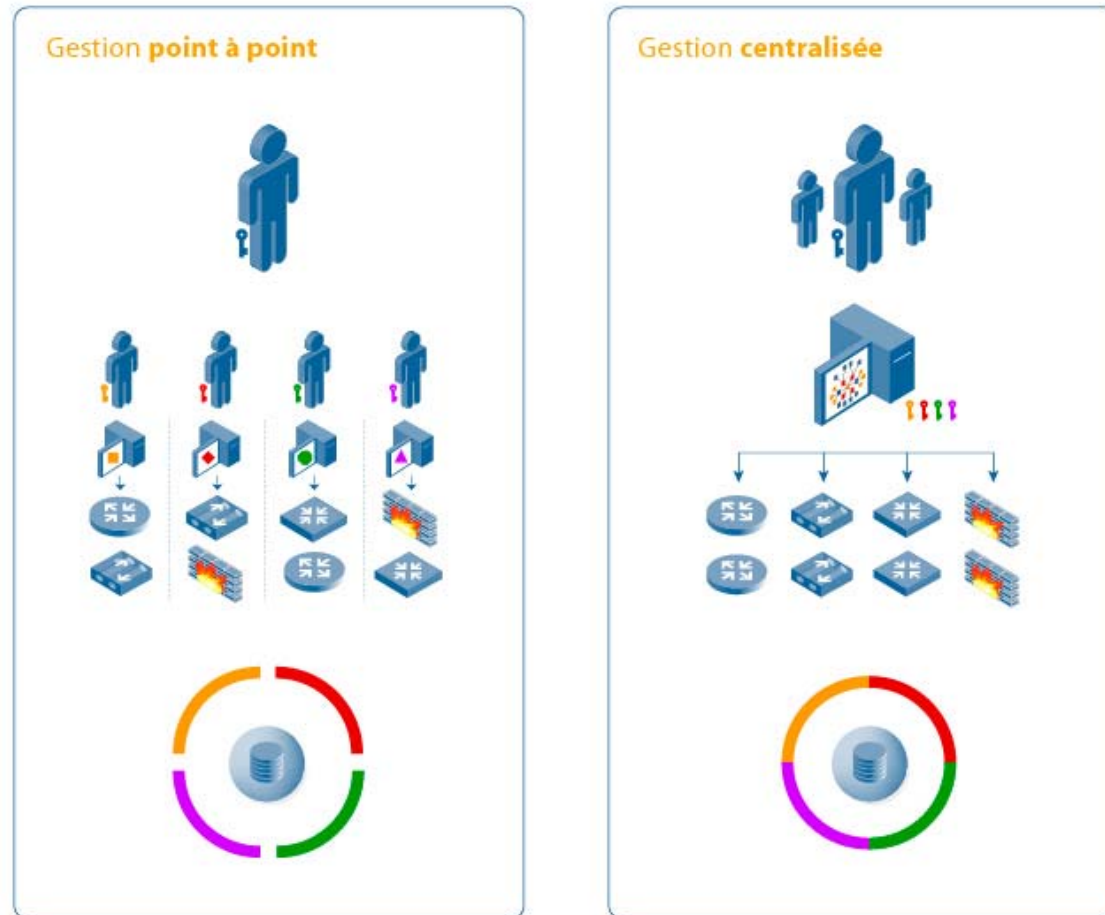
Routeurs



Commutateurs

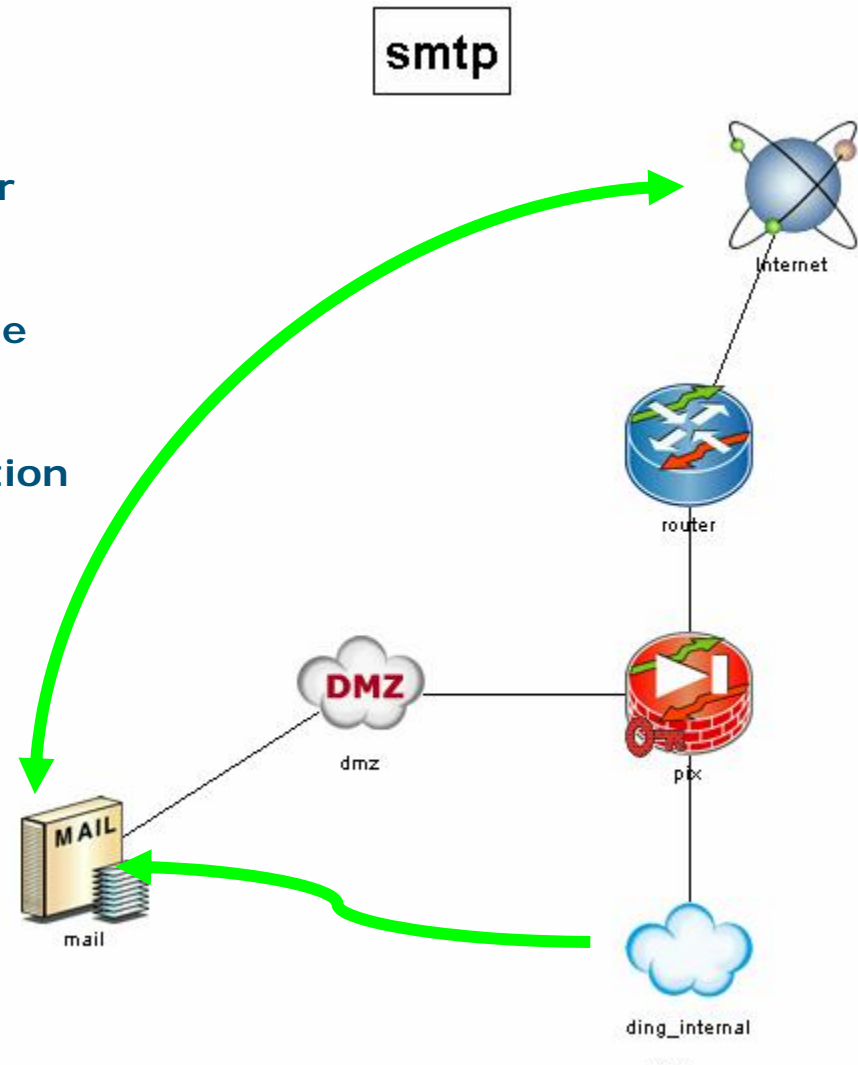




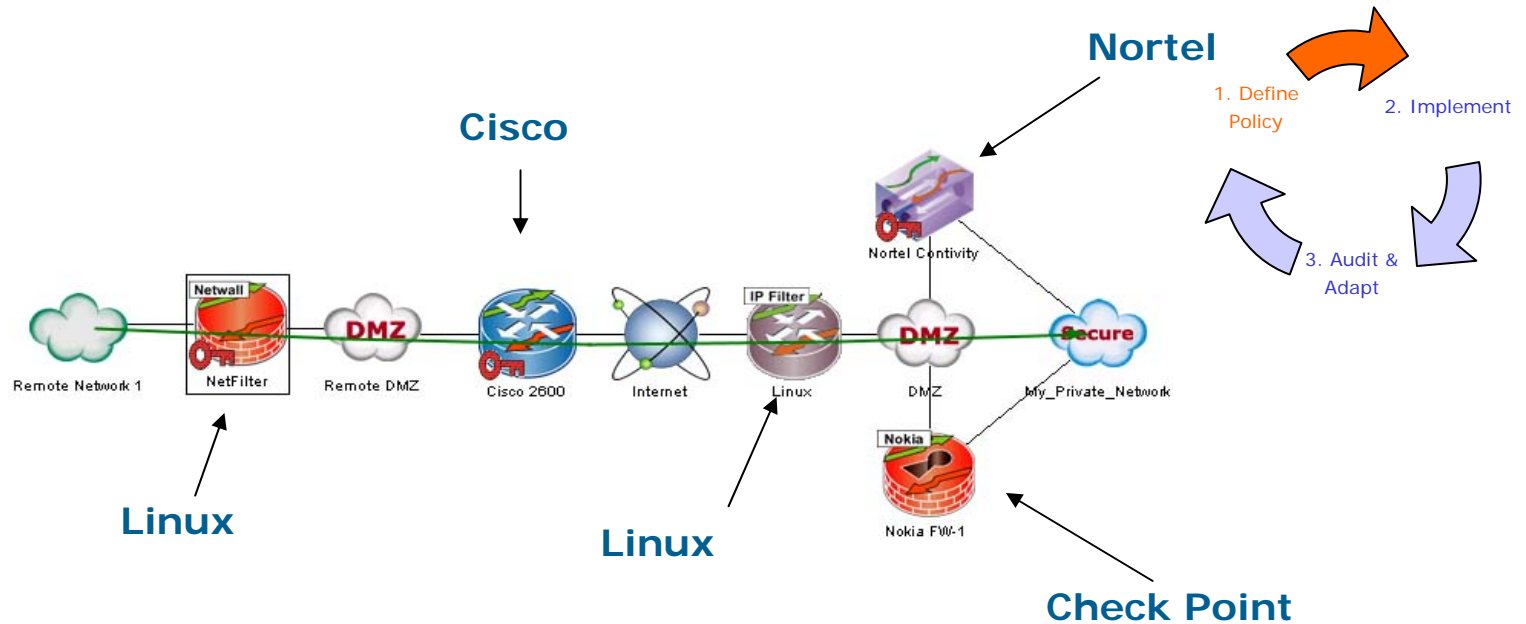


- Politiques de sécurité cohérentes à travers différents types d'équipements
- Gestion centralisée pour des marques multiples

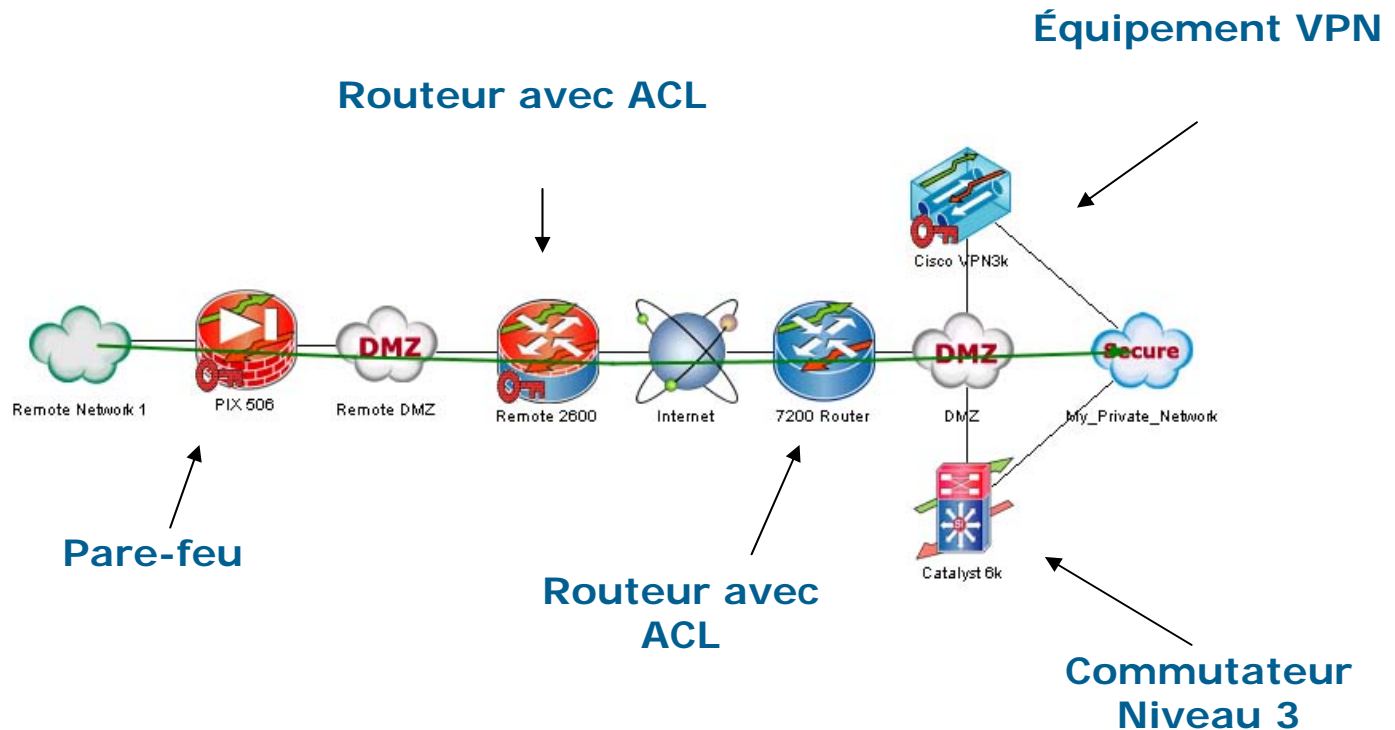
- Travailler uniquement sur les besoins fonctionnels.
- Exemple de diagramme de flux pour le flux SMTP
- Protocole de communication pour l'échange de mail



Définition de la politique : Un langage commun

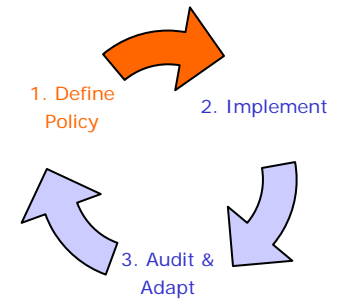


- Un design graphique pertinent
- Permet à tout le monde de parler le même langage
- Deny All – Permit Some
- Application de la politique de bout en bout



- **Travailler uniquement sur les besoins fonctionnels.**
 - Application des politiques de sécurité de « bout en bout »
- **Indépendante de la technologie des équipements**

- **Simplicité de la définitions des règles**
 - Vous dessinez des flèches
- **Multi-vendeurs**
 - CISCO, NetScreen, CheckPoint, Nortel, ...
- **Qualité : Nous respectons les meilleurs pratiques promues par les experts du marché**
 - Deny all par default, anti-spoofing, protection des routeurs...
- **Automatisation de la création des règles**
 - Les experts sont là pour faire évoluer les politiques pas pour pallier les insuffisances des produits qu'ils utilisent
- **Collaboration**
 - Gestion de droit basé sur l'accès et les responsabilités
 - Les équipes Sécurité et Réseau peuvent communiquer
 - Assurer un reporting en phase avec la réalité de la politique implémentée



SOLSOFT SECURITY DESIGNER

Design network security with a user-friendly graphic interface.

SOLSOFT POLICY SERVER

State-of-the-art policy management solution.

SOLSOFT SECURITY REPORTER

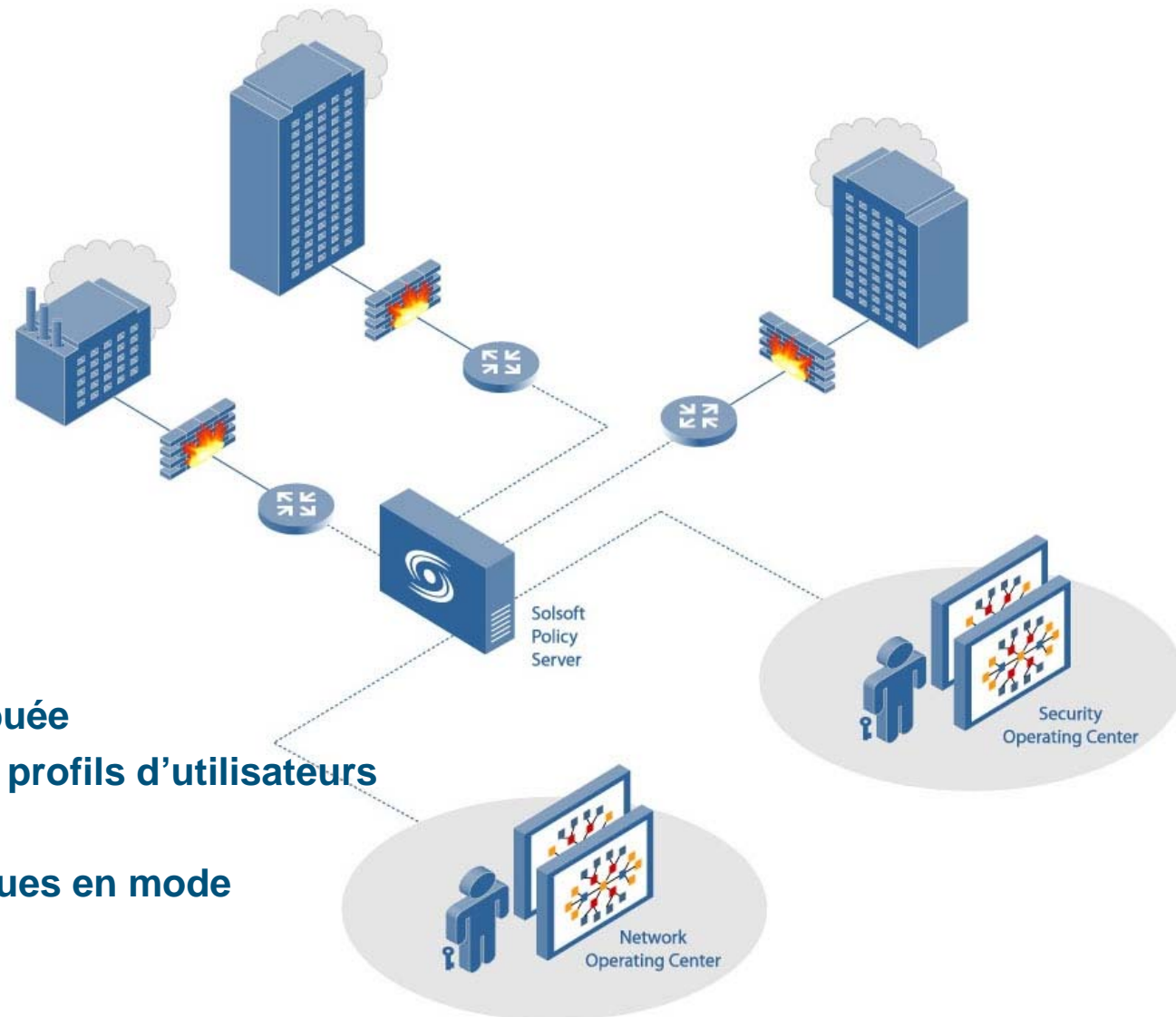
Web-based reporting for compliance and policy lifecycle management.

SOLSOFT TECHNOLOGY PACKS

Easily control your choice of security devices.



- **Importation des configurations à partir de HP Open View**
- **Importation des configurations de pare-feu de différents fournisseurs**
 - Objets
 - Adresses IP
 - Règles de sécurité
- **Migration simple d'une marque à l'autre**
 - Changez les propriétés de l'équipement dans Solsoft Security Designer.
 - Génération automatique de la configuration dans le langage natif du nouvel équipement cible.



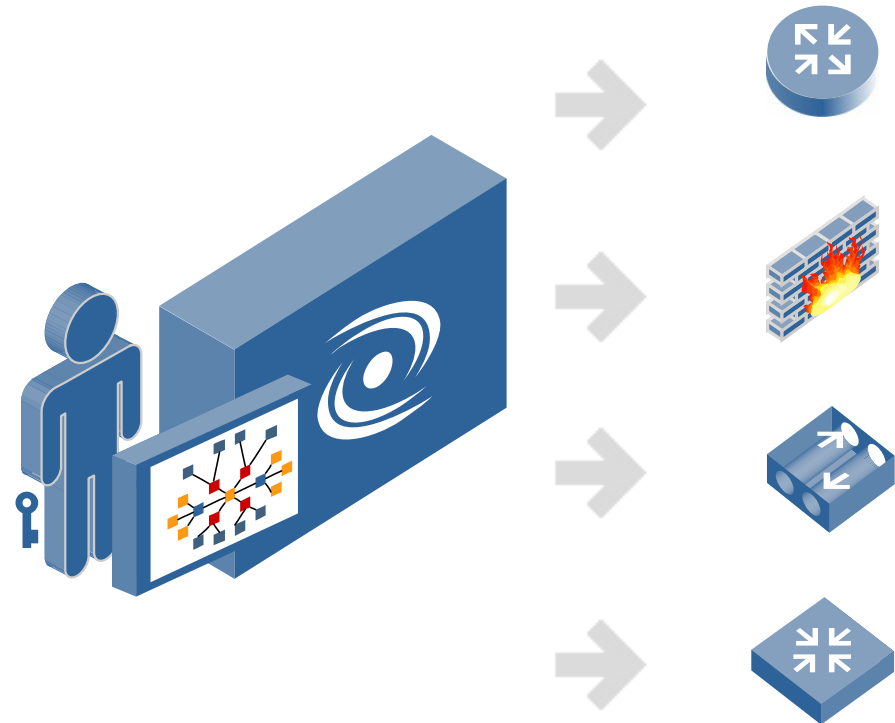
- **Architecture distribuée**
- **Administration des profils d'utilisateurs**
- **Profils Granulaires**
- **Gestion des politiques en mode workflow**

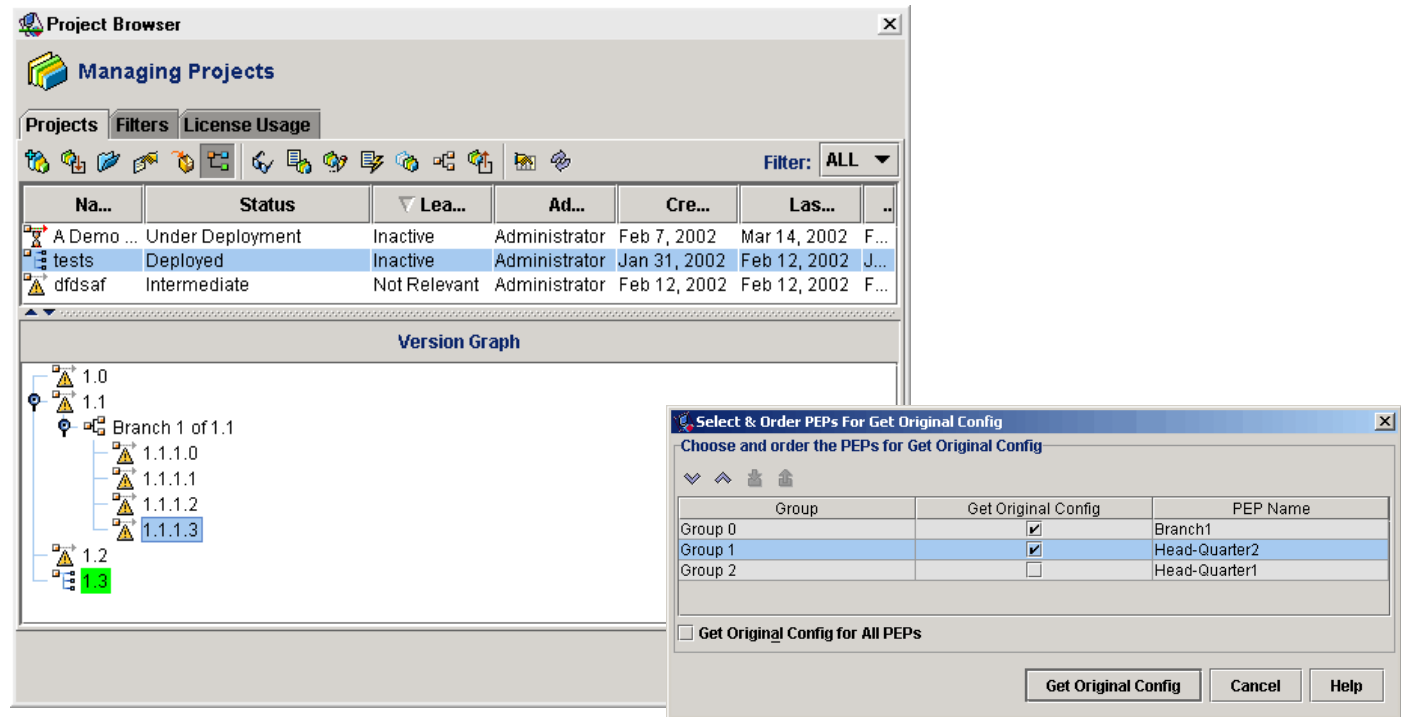
• **Changement des règles**

- Mise à jour simple et facile
- Calcul automatique des nouvelles politiques

• **Téléchargement**

- Sécurisé et vérification du chemin
- Automatique sur les équipements cibles
- Retour à des configurations précédentes (fonction « Roll-Back »)
- Classification par groupes d'objets
- Rapport et log en continu





The screenshot shows the 'Project Browser' window with a table of projects and a 'Version Graph' tree. A dialog box titled 'Select & Order PEPs For Get Original Config' is open, showing a table for selecting configurations.

Group	Get Original Config	PEP Name
Group 0	<input checked="" type="checkbox"/>	Branch1
Group 1	<input checked="" type="checkbox"/>	Head-Quarter2
Group 2	<input type="checkbox"/>	Head-Quarter1

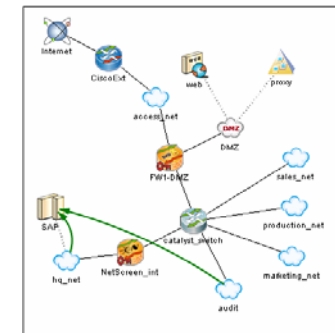
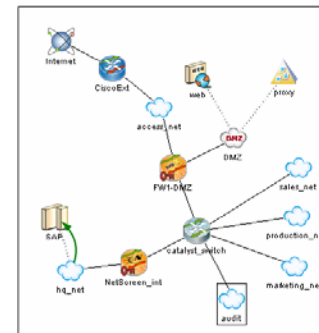
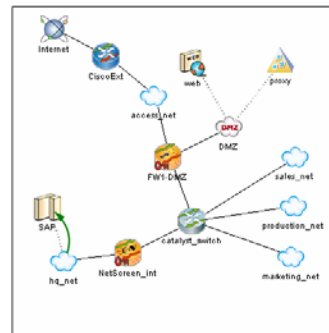
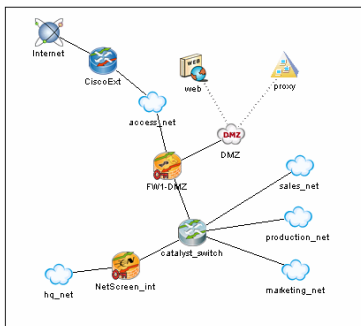
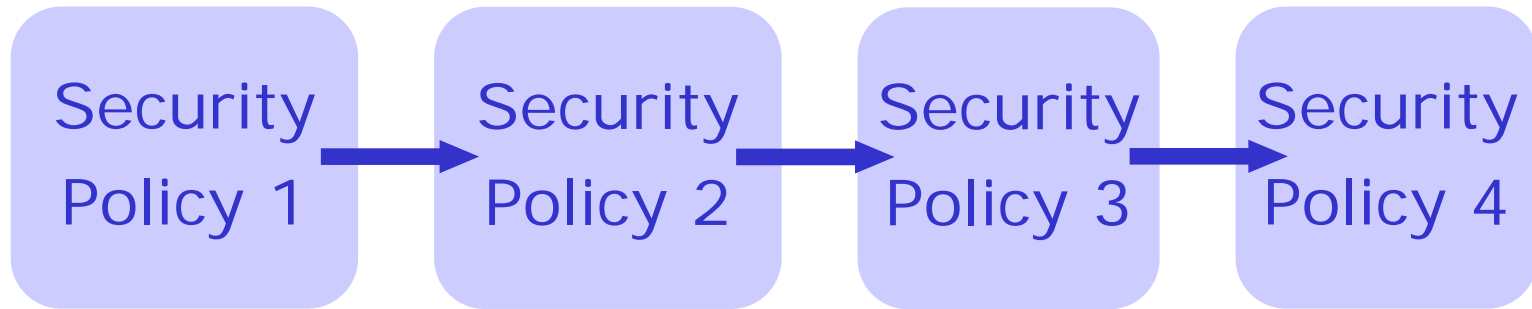
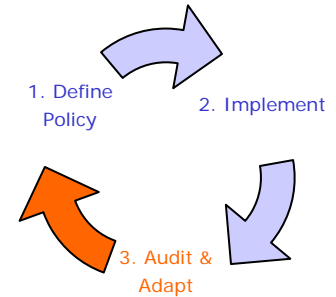
Get Original Config for All PEPs

Buttons: Get Original Config, Cancel, Help

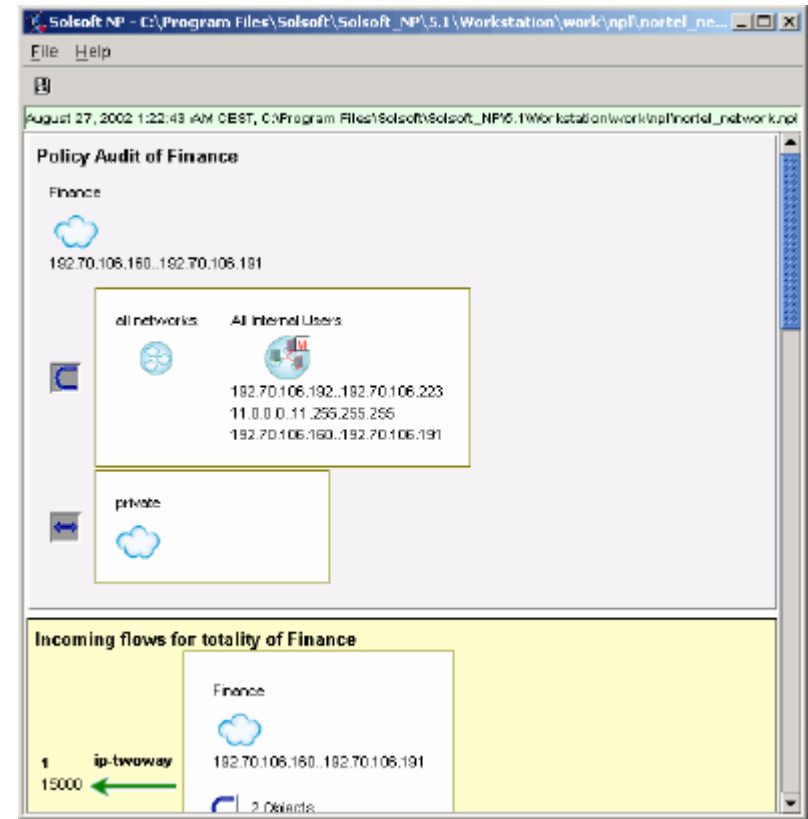
- Tous les changements de politiques sont sauvegardés
- Commentaires et procédure aident à la collaboration
- Déploiement et retour en arrière sur n'importe quelle configuration à n'importe quel moment
- Flexibilité et simplicité sont des moteurs de changements
- Des scénarios prévisionnels peuvent être construits, simulés et déployés rapidement
- Pas de divergence entre le cahier des charges et le résultat sur les équipements

Adapter et Auditer : La gestion dans le temps sans divergence

- Une vision claire de l'évolution des politiques
- Pas de divergences entre politique papier et configurations des équipements
- Travail collaboratif



- **L'audit des politiques est conduit sur l'intégralité du réseau...**
- **...quel que soit l'objet**
 - Adresse IP
 - Policy Enforcement Point
 - Intégralité du réseau
- **Les configurations NAT et les règles d'acheminement (path restriction) sont prises en compte**
- **Conseils et aide pour la gestion de vulnérabilités potentielles**



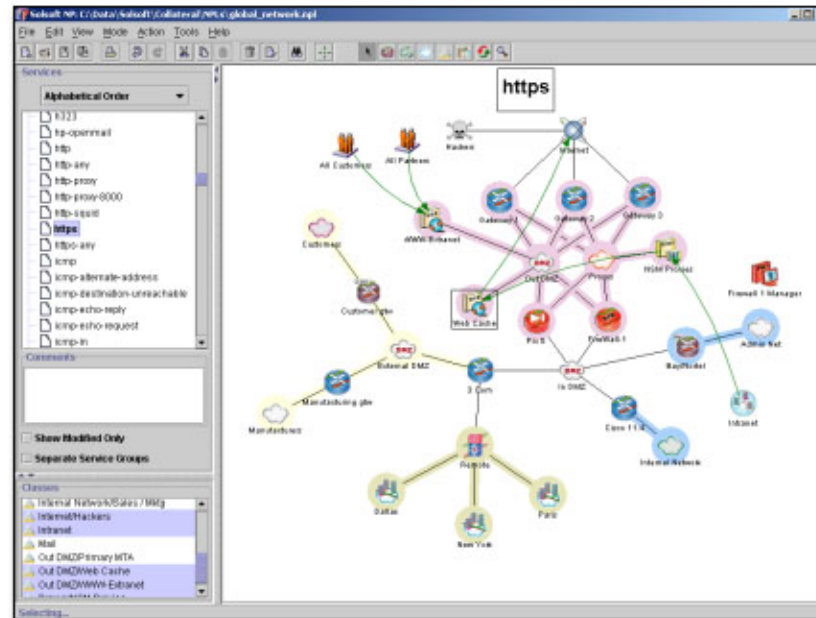
The screenshot displays the Solsoft NP interface for a 'Policy Audit of Finance'. The window title is 'Solsoft NP - C:\Program Files\Solsoft\Solsoft_NP\5.1\Workstation\work\ntp\nortel_ne...'. The main content area shows a tree view with 'Finance' selected. Under 'Finance', there are three sub-items: 'all networks', 'All Internet Users', and 'private'. The 'all networks' item is expanded, showing a cloud icon and the IP range '192.70.106.160..192.70.106.191'. The 'All Internet Users' item is also expanded, showing a globe icon and the IP ranges '192.70.106.192..192.70.106.223', '11.0.0.0..11.255.255.255', and '192.70.106.160..192.70.106.191'. The 'private' item is collapsed, showing a cloud icon. Below the tree view, there is a section titled 'Incoming flows for totality of Finance' with a yellow background. It shows a table with one entry: '1 ip-twoway 15000' with a green arrow pointing left. To the right of this entry is a box containing a cloud icon and the IP range '192.70.106.160..192.70.106.191'. The bottom right corner of the interface shows '2 Objects'.

- Interface Web
- Un tableau de bord de la sécurité des réseaux
- Un moteur de requête
 - Troubleshooting
 - Audits de Sécurité
 - Reporting automatique
- Facilite la conduite de changement et la séparation des tâches entre plusieurs équipes

The screenshot displays the Solsoft Security Reporter web interface. At the top, there is a navigation bar with tabs for DASHBOARD, SECURITY POLICY, REPORTS, and TASKS. Below this, there are sub-tabs for Deployment, Assets, Rules, and Search. The current page is titled 'security policy > rules'. The main content area shows 'Rules' with a search results section. The search criteria are: Type: ALL, Service: ALL, Source: ALL, Destination: ALL. The display options are: Object names, Object IP, Explicit Rules, Implicit Rules. The results are sorted by 'Services'. A table lists the rules with columns for ID, Source, Destination, Service, Type, Paths, Category, and Flow properties. The table contains 18 rows of data.

ID	Source	Destination	Service	Type	Paths	Category	Flow properties
<input type="checkbox"/> 145	GWAY1.acme-corp.com	GWAY1.acme-corp.com	telnet	allow	4 (view)		
<input type="checkbox"/> 146	GWAY2.acme-corp.com	GWAY2.acme-corp.com	telnet	allow	3 (view)		
<input type="checkbox"/> 147	myPEP3.acme-corp.com	SPS.acme-corp.com	ftp	allow	4 (view)		
<input type="checkbox"/> 369	myPEP4.acme-corp.com	myPEP4.acme-corp.com	ftp	deny	1 (view)		
<input type="checkbox"/> 290	SPS.acme-corp.com	myPEP4.acme-corp.com	telnet	deny	5 (view)		
<input type="checkbox"/> 146	GWAY2.acme-corp.com	GWAY2.acme-corp.com	telnet	allow	3 (view)		
<input type="checkbox"/> 147	myPEP3.acme-corp.com	SPS.acme-corp.com	ftp	allow	4 (view)		
<input type="checkbox"/> 369	myPEP4.acme-corp.com	myPEP4.acme-corp.com	ftp	deny	1 (view)		
<input type="checkbox"/> 155	GWAY1.acme-corp.com	GWAY1.acme-corp.com	telnet	allow	4 (view)		
<input type="checkbox"/> 146	GWAY2.acme-corp.com	GWAY2.acme-corp.com	telnet	allow	3 (view)		
<input type="checkbox"/> 157	myPEP3.acme-corp.com	SPS.acme-corp.com	ftp	allow	4 (view)		
<input type="checkbox"/> 146	GWAY2.acme-corp.com	GWAY2.acme-corp.com	telnet	allow	3 (view)	implicit upload flow	view details
<input type="checkbox"/> 45	GWAY1.acme-corp.com	GWAY1.acme-corp.com	telnet	allow	4 (view)		
<input type="checkbox"/> 46	GWAY2.acme-corp.com	GWAY2.acme-corp.com	telnet	allow	3 (view)		
<input type="checkbox"/> 147	myPEP3.acme-corp.com	SPS.acme-corp.com	ftp	allow	4 (view)		
<input type="checkbox"/> 369	myPEP4.acme-corp.com	myPEP4.acme-corp.com	ftp	deny	1 (view)		

- **Démonstration produit**





Services

Alphabetical Order

- ah
- any
- aol
- ap-defender
- archie
- at-defender
- backweb
- bgp
- biff
- bootp-broadcast
- bootp-relay
- cachefs
- cifs
- cmsd
- connectedonline
- cooltalk
- cooltalk

Show Used Only

All Services

Trust Zones

Relevant Objects

- all networks
- all PEPs
- Solsoft Client
- Solsoft Server

any

Add Network



- **Vidéo clip d'une session d'Upload**
- **En vitesse réelle**
- **La méthode d'Upload est SSH**
 - Communication sécurisée – état de l'art actuel
 - Peut être configuré pour TFTP comme pour un protocole plus lent et moins sécurisé comme telnet
- **Les cibles d'Upload**
 - Un ou 100, cela ne change rien
 - Équipements similaires ou différents, cela ne change rien non plus



Services

Alphabetical Order

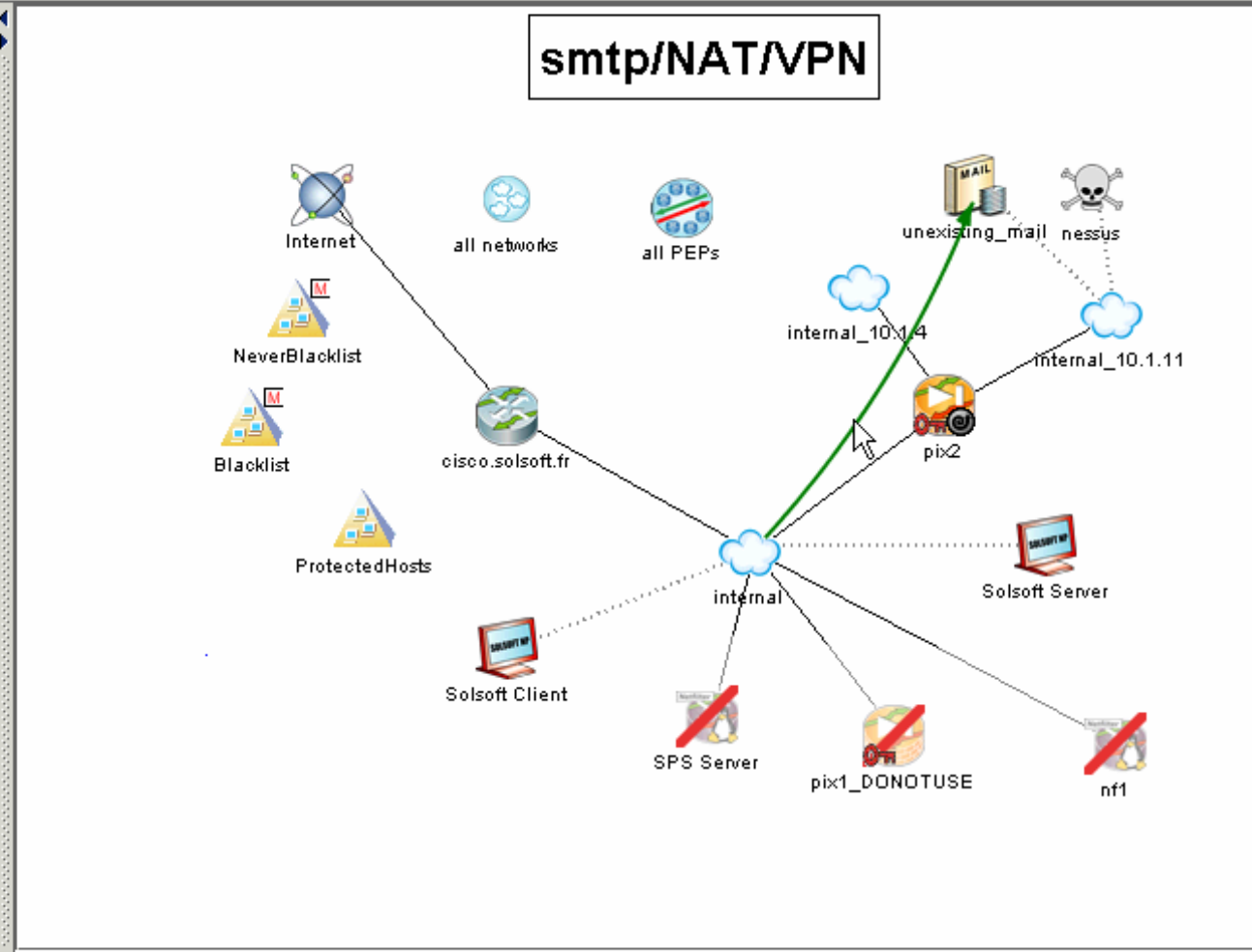
- any
- http
- http-proxy
- https
- ping
- smtp
- snmp
- solsoft_np
- ssh
- telnet
- tftp

Show Used Only

All Services

Relevant Objects | Trust Zones

- all networks
- all PEPs
- Blacklist
- internal
- Solsoft Client



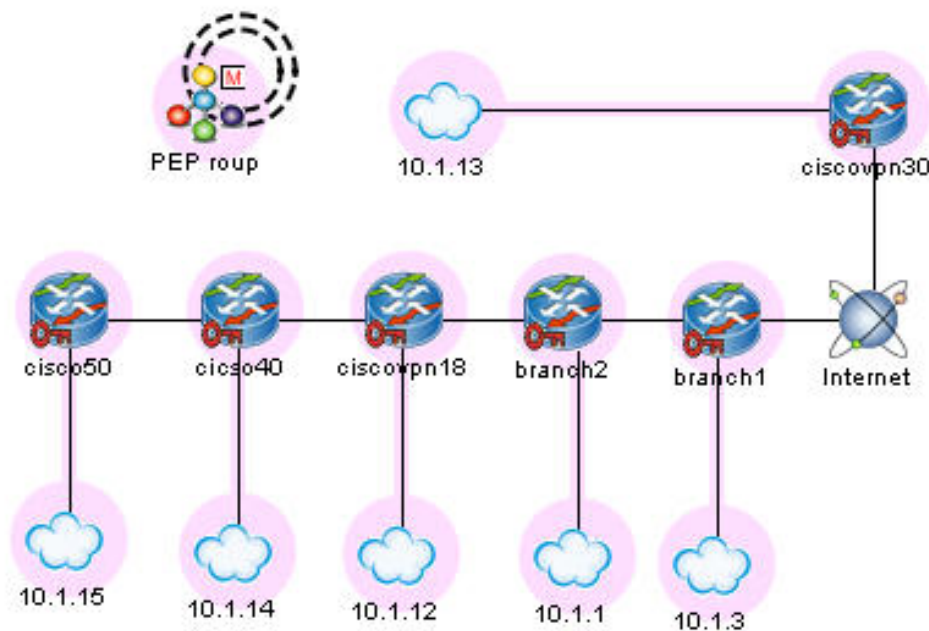
```

[INFO]pix2(config)#
[INFO]pager 24
[INFO]
[INFO](successful).
[INFO]### Finished action on PEP pix2 ###
    
```

- **Pas de problèmes d'échelle**
 - Upload une centaine d'équipements sans problème
- **Diminue le risque lors de la configuration**
 - La configuration et l'upload manuel sont sujets à l'erreur humaine
 - Limite les temps de maintenance
 -
- **Multi-vendeur**
 - Pas d'apprentissage et de formation nécessaire pour un nouvel équipement
- **Bonne gestion des ressources**
 - On utilise les ressources limitées et de haute valeur pour l'expertise sécurité
 - Pas pour les tâches répétitives d'upload et de configuration
- **La défense en profondeur peut être maintenue**
 - Avec n'importe quel nombre d'équipement
 - Avec n'importe quelle profondeur de réseau
- **On peut effectuer très rapidement un "Roll Back" vers une bonne configuration**
 - Toujours possible
 - C'est un bon filet de sécurité

- **5 types de profils de sécurité**
 - Pas de filtrage (Anti-spoofing seulement)
 - Sécurité de l'équipement (Anti-spoofing + restriction des accès)
 - Filtrage en gros (Optimisé pour réduire la taille des filtres sur les backbones)
 - Filtrage « custom »
 - Filtrage Solsoft « Best Practice »
- **Permet de réduire la taille des filtres.**
- **Paramétrage simple pour s'adapter a la fonction de l'équipement**
 - Spécialisation du comportement de l'équipement
 - Évite d'être trop fin dans le filtrage
- **La politique de sécurité intègre aussi les choix d'optimisation**
 - Les choix sont donc gère au niveau de la politique et plus manuellement, équipement par équipement

- **Conception des VPNs par une représentation visuelle simplifiée**
 - Mettre en place un VPN “Fully meshed” ou “Hub and Spoke” se fait en quelques minutes
 - Optimise les configurations des tunnels automatiquement
 - Supporte la diversité des équipements et des fonctions avancées comme le DMVPN



Fully meshed VPN, avec 6 équipements, $6 \times 5 / 2 = 15$ tunnels

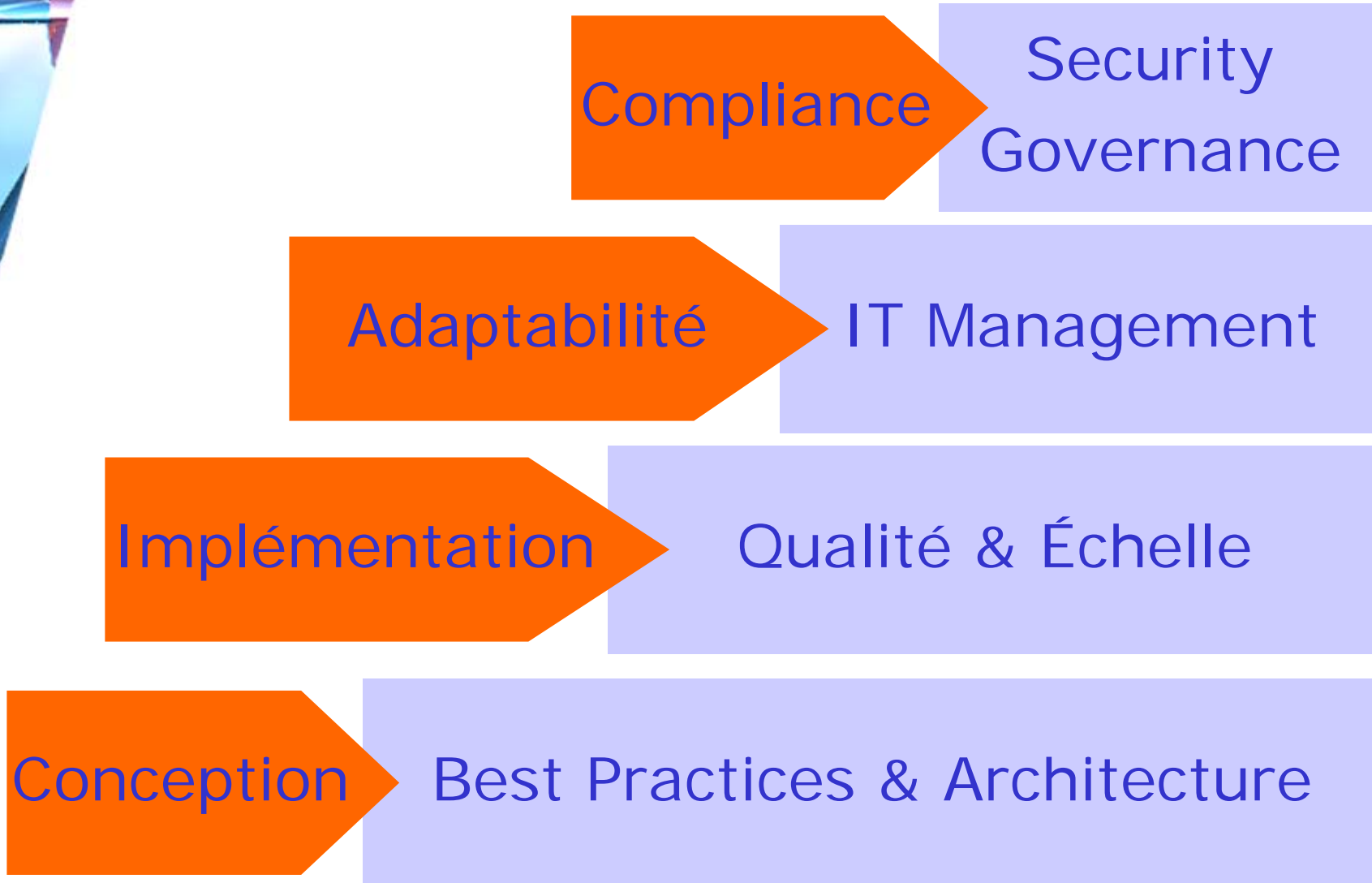
- **Solsoft travaille avec l'ensemble des acteurs du marché de la sécurité informatique**
- **Nous avons des partenariats actifs avec:**

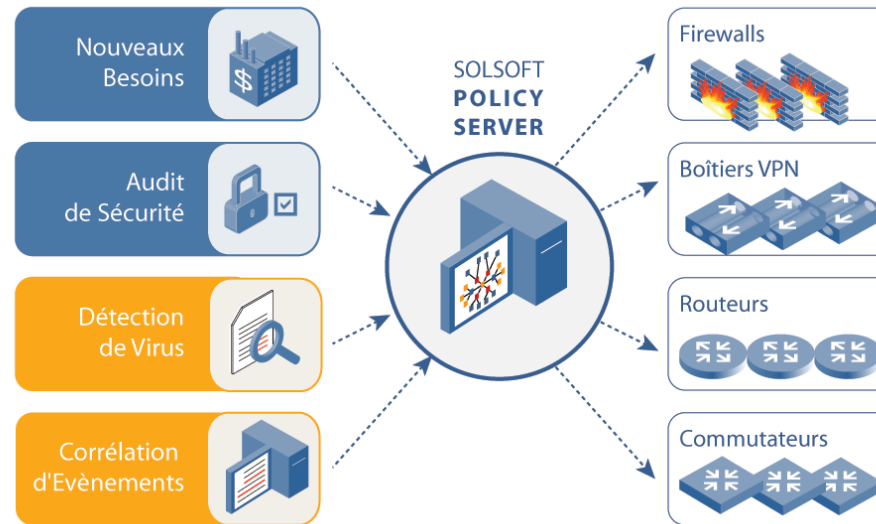
- ArcSight
- Astaro
- Cisco Systems
- Check Point
- Hewlett-Packard
- MicroMuse
- Network Intelligence
- NetScreen
- Nortel Networks
- Shiva
- Symantec



Evolutions produit

	FEATURES	DEVICES	
2004	<ul style="list-style-type: none"> Web-based reporting VPN tunnel grouping Scheduling services Configuration optimization Reporting engine 	<ul style="list-style-type: none"> Check Point NG AI Juniper Networks NetScreen 5 Nortel Networks Alteon Firewall Cisco VPN3000 4.1 Cisco FWSM 2.2 	v6.0
2003	<ul style="list-style-type: none"> Virtual Systems support VPN Client to Gateway Web Services API PKI enablement Cluster management 	<ul style="list-style-type: none"> Check Point NG Symantec EF Astaro Cisco Catalyst VPNSM NetScreen VPN 	v5.3
2002	<ul style="list-style-type: none"> Server based architecture Multi-user management Role-based management Policy versioning 	<ul style="list-style-type: none"> Nortel Networks Contivity Cisco PIX 6.x NetScreen Firewall Cisco Catalyst FWSM 	v5.0
2001	<ul style="list-style-type: none"> Policy learning mode Firewall rule import Device SDK 	<ul style="list-style-type: none"> NetFilter Cisco VPN3000 Intel NetStructure 	v4.3
2000	<ul style="list-style-type: none"> IPsec VPN support Visual global NAT configuration 	<ul style="list-style-type: none"> Check Point Firewall-1 4.x Cisco PIX 5.x 	v4.0
1999	<ul style="list-style-type: none"> Support for Network Address Translation HP Open View Import 	<ul style="list-style-type: none"> Cisco PIX Firewall 4.x Nortel Networks BayRS Cisco IOS Firewall, IOS 12.x 	v3.2
1998	<ul style="list-style-type: none"> Visual interface representing Network Policy Policy audit by global analysis 	<ul style="list-style-type: none"> StorageTek BorderGuard Bull NetWall 3.0 	v3.0
1997	<ul style="list-style-type: none"> Network Policy Language Device configuration generator 	<ul style="list-style-type: none"> Cisco IOS 9.21,10,11 IP Filter, IP Chains, IP Firewall 	v2.0



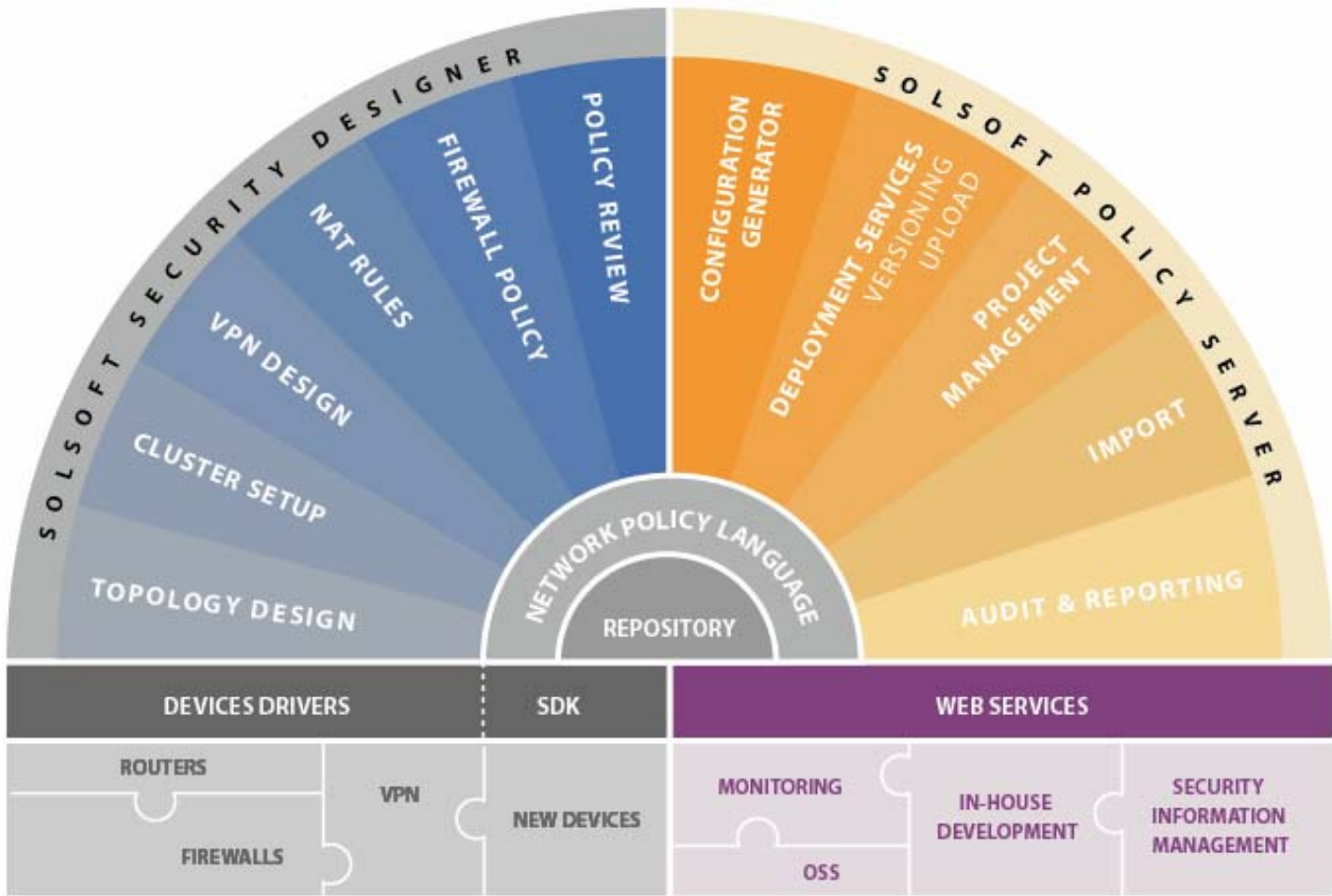


- **Solsoft Policy Server API**

- Interopérabilité avec d'autres logiciels
 - Monitoring
 - Corrélation d'évènements
 - OSS
 - Applications de Support i
 - Autres applications internes
- Technologie Web Service

- **Solsoft Device SDK**

- SDK utilisé en interne
- Outils + formation
- Programme de certification
- Intégration courte de nouveaux équipements





- Unified management for a Cisco and Check Point security environment with VPN 3000, IOS VPN, PIX FWSM Blade and Firewall-1 with more than 50 devices.
- Selection Criteria
 - Multi-vendor (partnerships)
 - Mapping / end-to-end enforcement / scalability
 - Process driven enabling SLAs
- Solsoft Solution
- “Without centralized and graphical management, it was impossible to develop end-to-end policies that worked for our network. We needed a solution bringing powerful design of policy all the way to deployment.”
- **Amar Saoudi, Security Administrator – Caisse d'Epargne**

- **Challenge**

- Trouver une solution qui puisse gérer l'ensemble de leurs équipements Cisco à partir d'une interface unique et simple. Besoin de gérer des PIX, 2600 Routers avec des ACL et du VPN IPsec.
- Voulaiient une flexibilité qui permette d'utiliser le produit pour gérer des équipements de marques différentes afin de ne pas avoir à former les opérateurs à plusieurs solutions dans l'avenir.

- **La solution Solsoft**

- Solsoft Policy Server permet d'avoir une gestion centralisée de la sécurité pour les routeurs Cisco IOS (FW and VPN), PIX FW, VPN 3000, et les switchs Catalyst.
- Le support de Solsoft pour d'autres vendeurs tels que Check Point, Netscreen and Nortel donne à Unisys/TSA la flexibilité nécessaire pour gérer la mise en oeuvre de la sécurité pendant les années à venir

- **Challenge**

- Dow Jones voulait consolider le nombre de ses firewalls, utiliser un nombre plus réduit de machines à haut débit. Pour cela, ils devaient trouver une solution de management simple qui puisse gérer l'ensemble de leurs équipements NetScreen, Cisco PIX, Check Point FW-1 and Nortel Contivity et rendre possible des processus de migrations technologiques pour l'équipe NOC.

- **Critères de sélection**

- Pouvoir supporter un nombre d'équipements qui croit, multi-vendeur, simple, basé sur des rôles et qui puisse s'adapter aux évolutions de l'entreprise

- **La Solution Solsoft**

- Dow Jones & Company a choisi Solsoft Policy Server pour configurer et gérer la sécurité sur l'ensemble de l'infrastructure de sécurité qui relie leurs divisions aux clients connectés en Extranet

- **Challenge**

- Veritas avait besoin d'une solution unifiée de gestion pour l'ensemble de son déploiement Cisco au niveau global dont les équipements sont : VPN 3000, IOS VPN, PIX FW/VPN 525.

- **Critères de sélection**

- Solution qui s'adapte à l'évolution de leur besoins, facile à utiliser, multi-vendeur (pour des choix ultérieurs d'équipements).

- **Solsoft Solution**

- "La gestion préventive du risque et la mise en conformité sont des soucis de première importance pour nous. Nous avons standardisé notre entreprise sur Solsoft Policy Server parce que le produit permet de simplifier les tâches de gestion des politiques de sécurité et la configuration des équipements. Notre équipe de sécurité globale utilise les fonctionnalités de gestion des rôles de Solsoft Policy Server pour gérer de manière collaborative l'ensemble de nos déploiements critiques de Firewall"

- **Greg Valdez, CIO at VERITAS**

Problèmes de gestion des politiques de sécurité

Pas de centralisation du contrôle de la politique

Manager un grand réseau ou un réseau hétérogène est coûteux et complexe

Les processus manuels sont coûteux en temps

Aucune interaction entre différents produits impacte la qualité et la productivité



SOLSOFT POLICY SERVER

Centralisé

Réduit les coûts

Automatisation et travail collaboratif

Multi-vendeur

SOLSOFT POLICY SERVER BENEFICES

SECURITE COHERENTE

AUTOMATISATION DES
PROCESS MANUELS

MULTI PATEFORME

MEILLEUR CONTROLE DE
LA SECURITE

SOLUTION OUVERTE



IMPACT SUR LE ROI

MOINS DE RISQUES

MOINS DE FORMATIONS
MOINS D'ERREURS

PLUS DE CHOIX
TECHNOLOGIQUE

AUDIT ET DOCUMENTATION
AUTOMATIQUES

IMPLEMENTATION ET
INTEGRATION RAPIDE



- **Pour plus d'informations :**

- www.solsoft.com

- **Philippe LANGLOIS**

Email: philippe.langlois_at_solsoft.com