HOW SECURE NETWORKS ARE MANAGED

Security Management of Large Networks and eXtreme Security Networks

SOLSOFT

PHILIPPE LANGLOIS

SR. SECURITY ARCHITECT
SECURITY RESEARCH LABS

XCON
Beijing, China -- September 2004

Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

Who We Are

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Solsoft provides organizations with the ability to centrally manage enterprise network security**
- **Goal**
  - Manage network security
  - Organize process in security provisioning
- **Benefits**
  - Makes network security more accurate, reliable and stable
  - Centralizes and automates policy creation and deployment
  - Lowers the cost and complexity of network security management

Who We Are

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Company**
  - Founded in 1997
  - Headquarters in Mountain View, California & Paris, France
  - Sales & Support in U.S & Europe
  - Over 200 customers worldwide

- **Largest European VC software funding in 2003**
  - €10 million = $12 million
    - The Carlyle Group (US)
    - Credit Lyonnais Asset Management (France)
    - Rotschild (France)
    - Logispring (Swiss)
  - Brings total to $32 million

- **Team of 70 includes former employees of**
  - Qualys, Cylink, Oracle, Cisco, Check Point, BMC, Microsoft, Computer Associates, ISS, HP,Network Associates…

Agenda

SOLSOFT

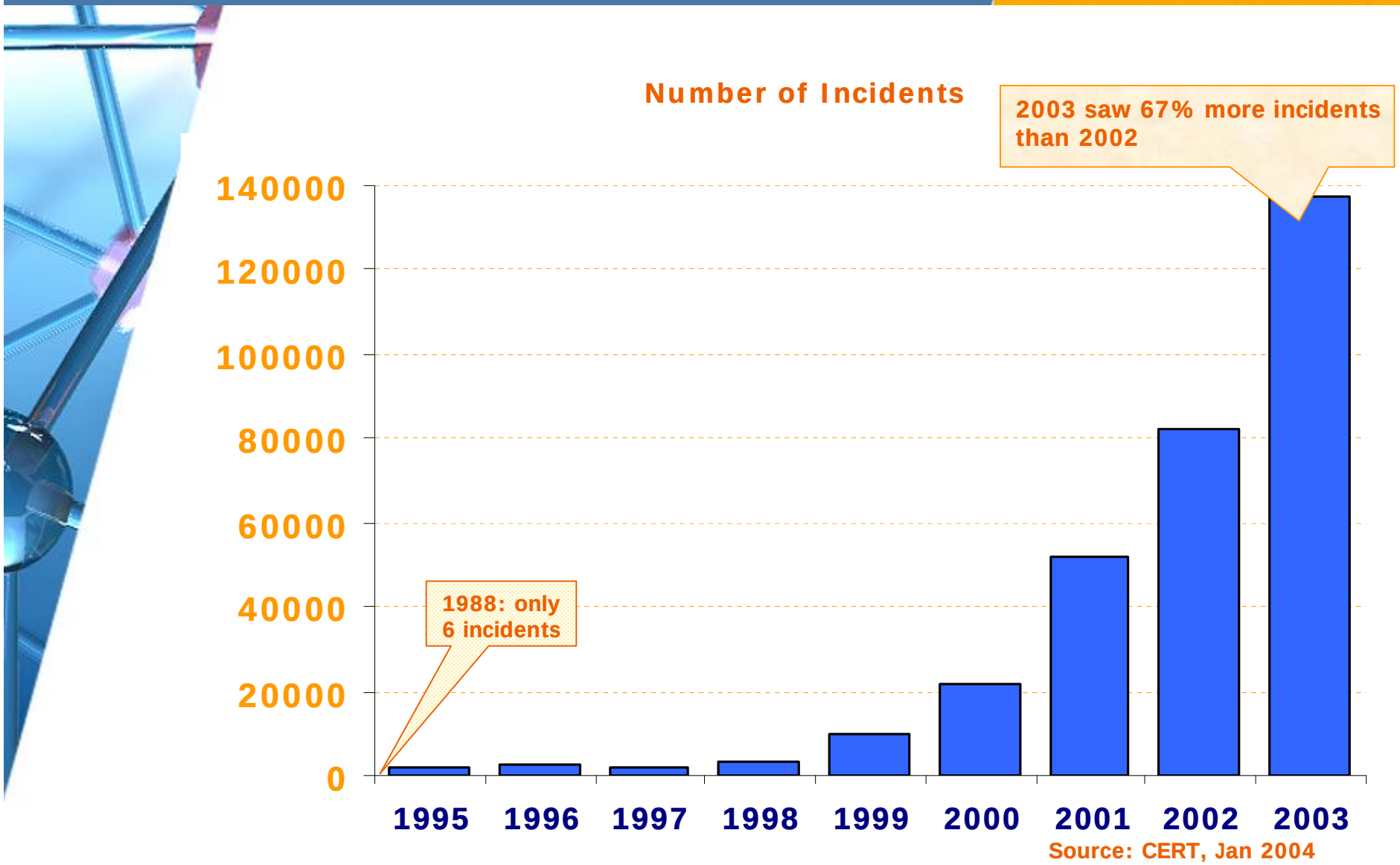
HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- **Security Context**
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

Increasing Security Threats

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Risk, Vulnerabilities and Threats

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

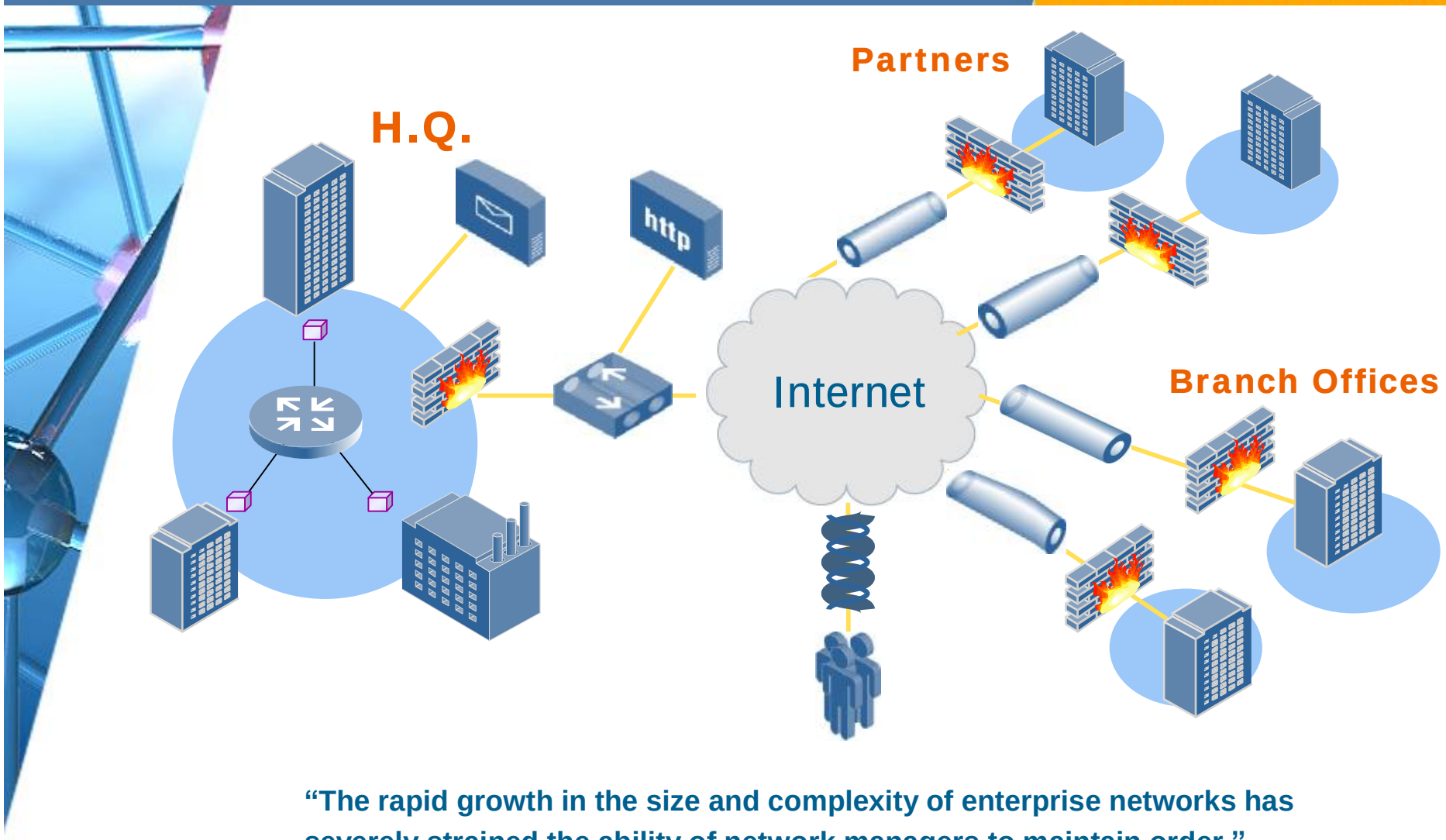
Risk = Vulnerability * Threat

- **The threat is ever increasing**
  - Number of Incidents from CERT
- **Vulnerabilities are being discovered continuously**
  - See bugtrap post as one factor
  - Top websites breached thanks to 0-days are another
  - Hard to evaluate
- **Thus Risk is HIGH!**

Growing Network Complexity

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



“The rapid growth in the size and complexity of enterprise networks has severely strained the ability of network managers to maintain order.”
- Forrester Research

Is my network secure ?

SOLSOFT

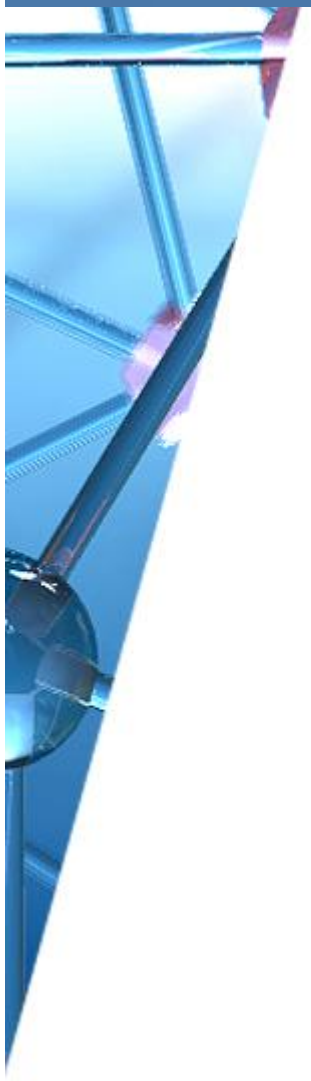
HOW SECURE NETWORKS ARE MANAGED

- What impact is this new business application going to have in my network ?
- What is the impact of network improvements and upgrades ?
- Do we really apply a common set of rules to all devices ? Are these up to date ?
- Can we quickly and globally adjust our security posture when new vulnerabilities are found ?
- Can we easily find what is currently deployed and working ?

Statements on the state of Security

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



"WE HAVE RECOGNIZED OVER THE LAST FEW YEARS THAT YOU CANNOT PREVENT A VIRUS."

- Joe Hartmann, director of North American antivirus research, Trend Micro

"SLAMMER SHOWED US THAT IT'S HARD FOR EVERYONE TO KEEP UP WITH PATCHES, NO MATTER WHO YOU ARE."

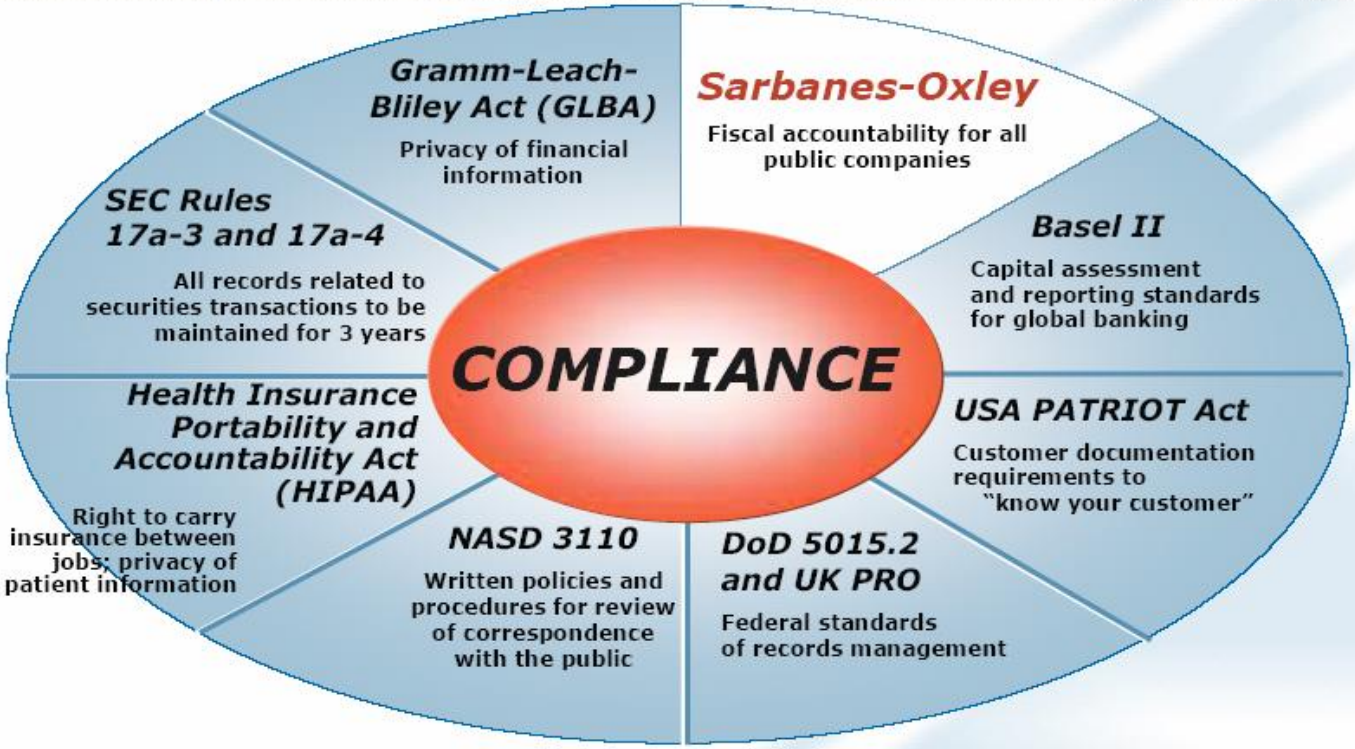
- Mary-Ann Davidson, chief security officer, Oracle

Compliance Pushes Security Management

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

The Compliance Landscape



Compliance initiatives are creating pressure on IT to ensure that the appropriate business support is in place

Source: META Group, April 2004

Network Security facts

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Automation leads to better Security**
  - More accurate
  - More reliable
  - More stable
- **Automation requires complex understanding**
  - Multi-brand fencing
  - Centralized management
  - Audit / reporting
  - Change management
- **Automation is the only way to ensure compliance and best practices:**
  - Audit and reporting on what is deployed and running
  - Centralized repository

Many Vendors Equipments…

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Cisco Systems | AVVID Partner

Juniper® Networks

ArcSight ESA Enterprise Security Alliance™

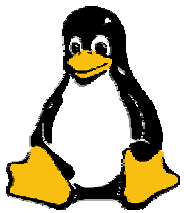
Check Point™ Software Technologies Ltd.

MicroMuse NetCool® Solutions

Nokia Connecting People

Network Intelligence Corporation

Nortel Networks



HP OpenView Portfolio Partner

HP OpenView Certified Application

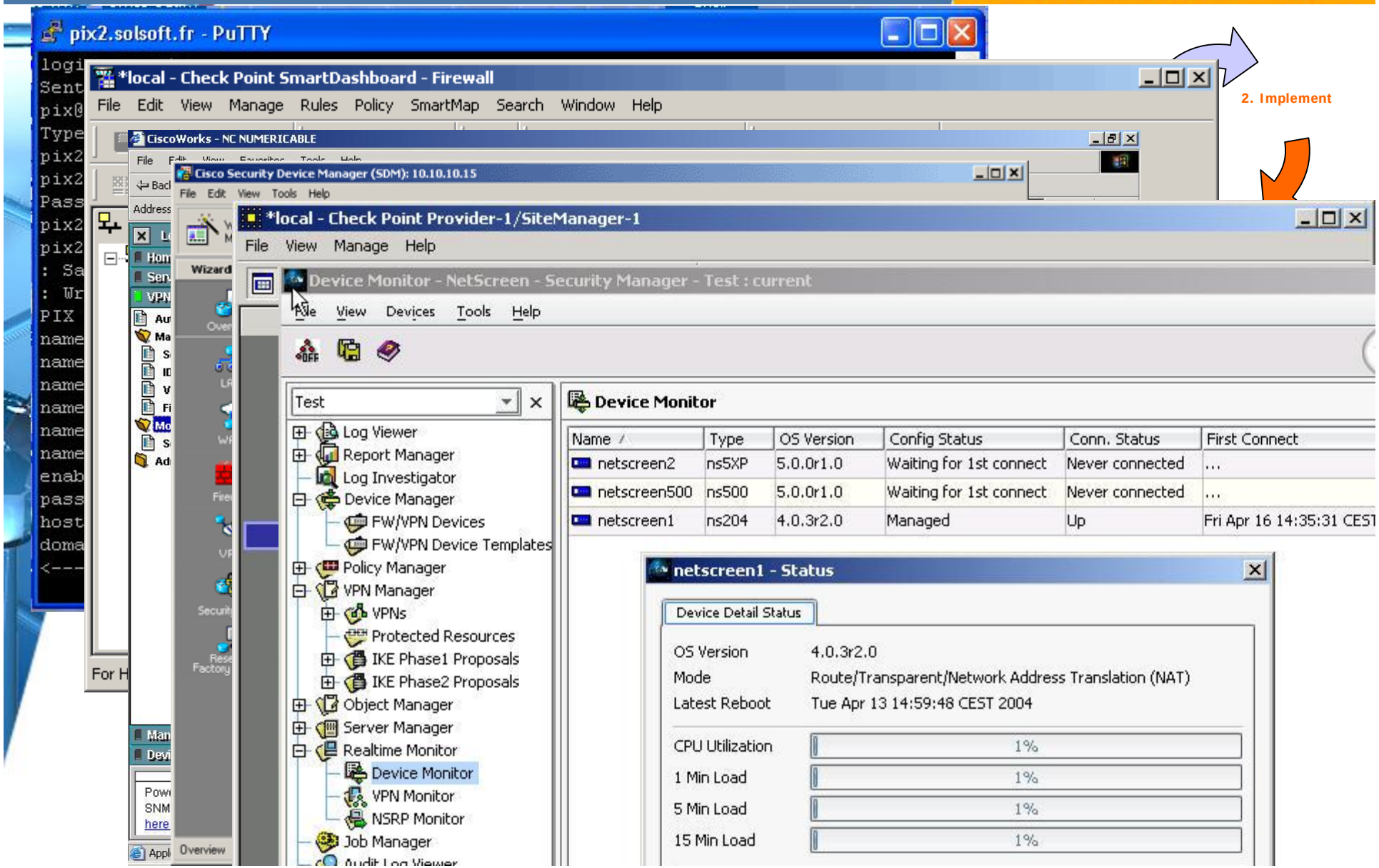
symantec.

astaro internet security

Many vendors configuration dialects!!!

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- **Solsoft Policy Server - Presentation and Demonstration**
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

The Network Security Challenge

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Business Requirements
- Security Audit
- Vulnerability Assessment
- Event Correlation

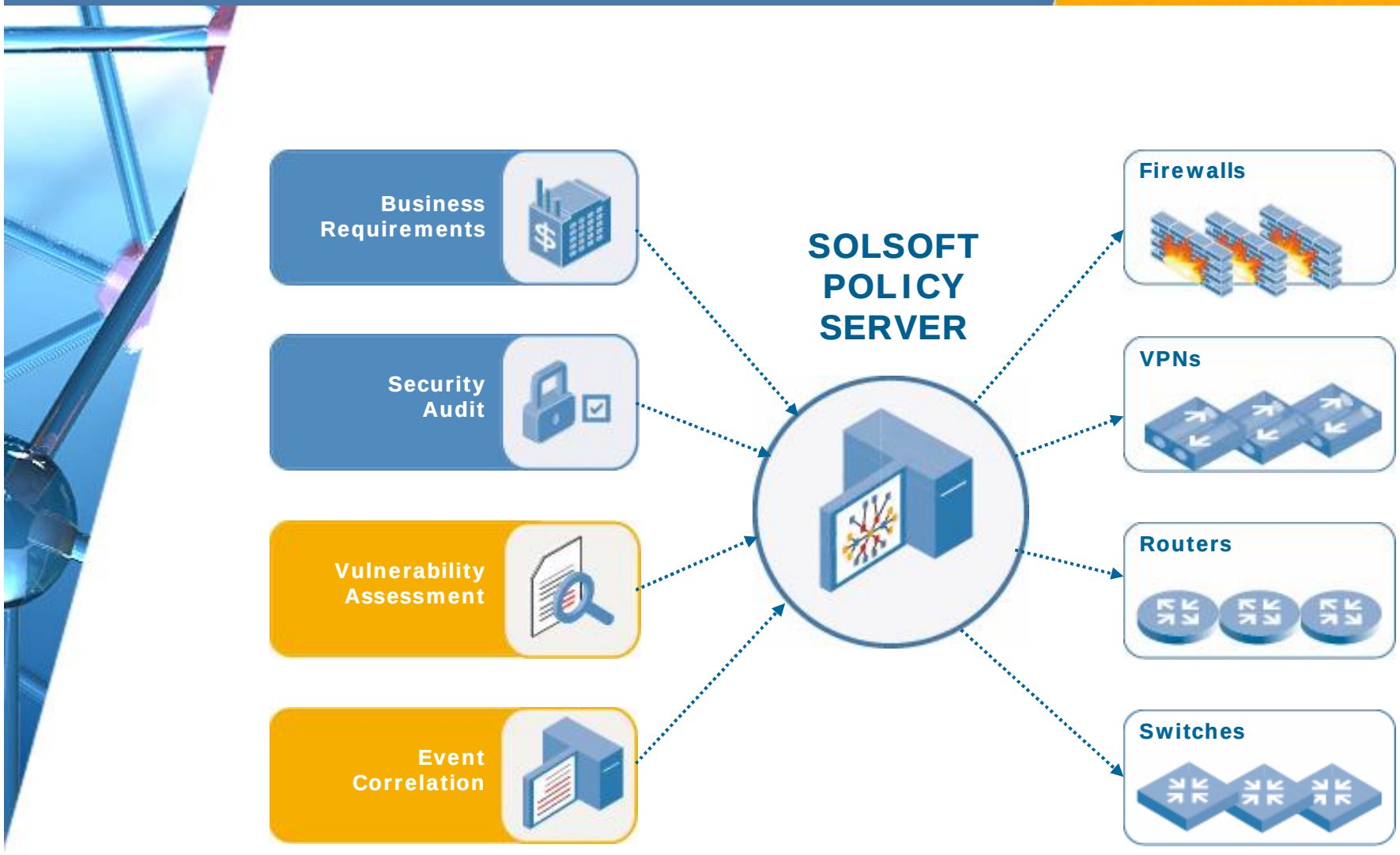
What's missing ?

- Firewalls
- VPNs
- Routers
- Switches

Where We Fit

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Expert Opinion

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

SPIRE security

“Managing network security configurations is often haphazard and random. Getting control over these configurations using an automated management solution like Solsoft's is the only way to manage the complexity of today's networks. The payoff is the ability to reduce risk through strategic exposure management.”

- Pete Lindstrom, Research Director, Spire Security

Solsoft enforce Best Practices in Security

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

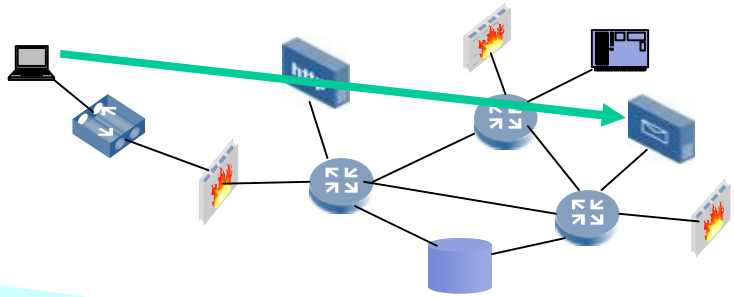
- **High level view -- centralized management**
  - Never get to do network management on one side
  - And power point job on the other side
- **Deny by default policy**
  - All traffic is denied by default
  - Only what is allowed goes through
- **Internal segmentation**
  - All routers on the path enforce deny by default
- **Secure the infrastructure**
  - PEPs – Policy Enforcement Points – are automatically configured to secure themselves from any external connection
- **Anti-spoofing**
  - We know the topology, thus we know where packets are supposed to be
  - Filtering to prevent packet injection

Model Based security

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Solsoft Security Model



Visual rule definition

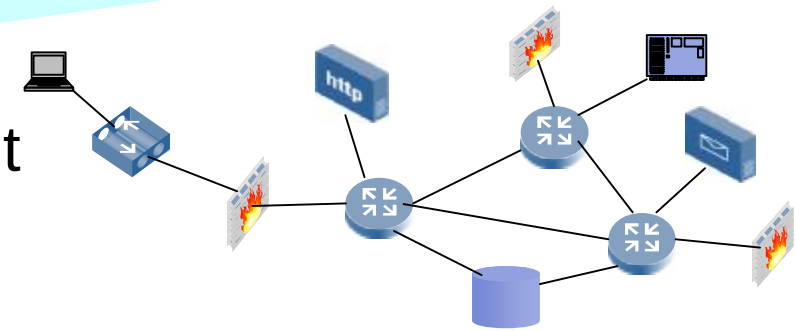
Simulations & checks

Deploy

Audit

Roll-back

Live Network Environment



Our Object Model of the Network

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

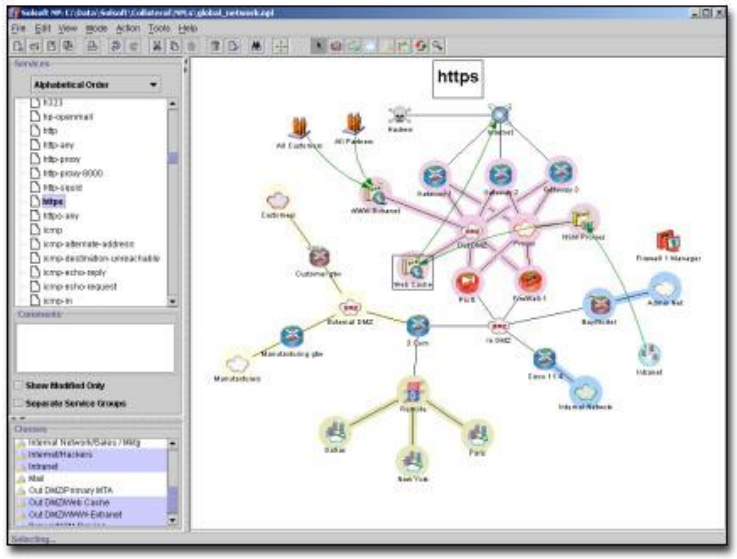
- **Solsoft Policy Server uses an Object Model to represent networks**
  - Modelize any kind of network
  - Store knowledge about topology
  - Understand different device types (NATs, VPNs, Clusters, HA)

- **Thus we can compile all the network flows into actual configuration**
  - Manual problem with best practices
    - Try to implement deny by default on 20 routers BY HAND
    - If you have only 50 flows, that means 1000 ACLs to write by hand.
    - To do that by hand means suicide!
    - That's why internal backbone rarely enforce ACLs
  - No problem to be redundant, the machine works for us
  - We manage hundreds of routers with deny by default best practice

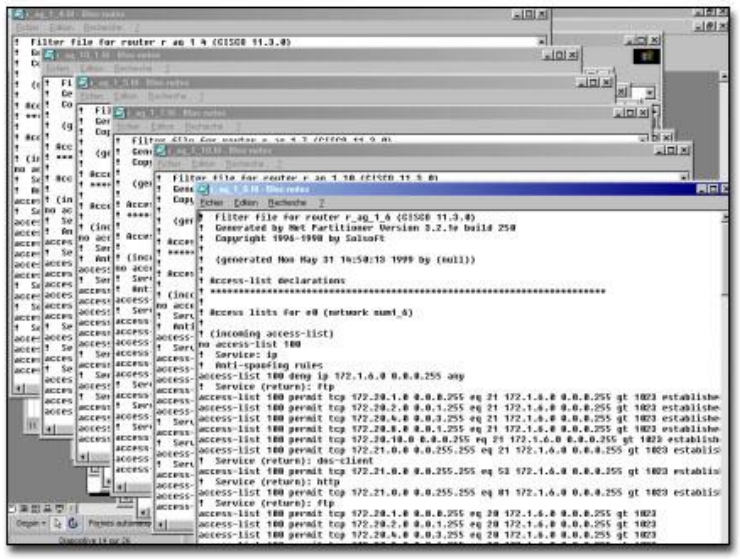
Powerful Visual Design

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Security Policy Design



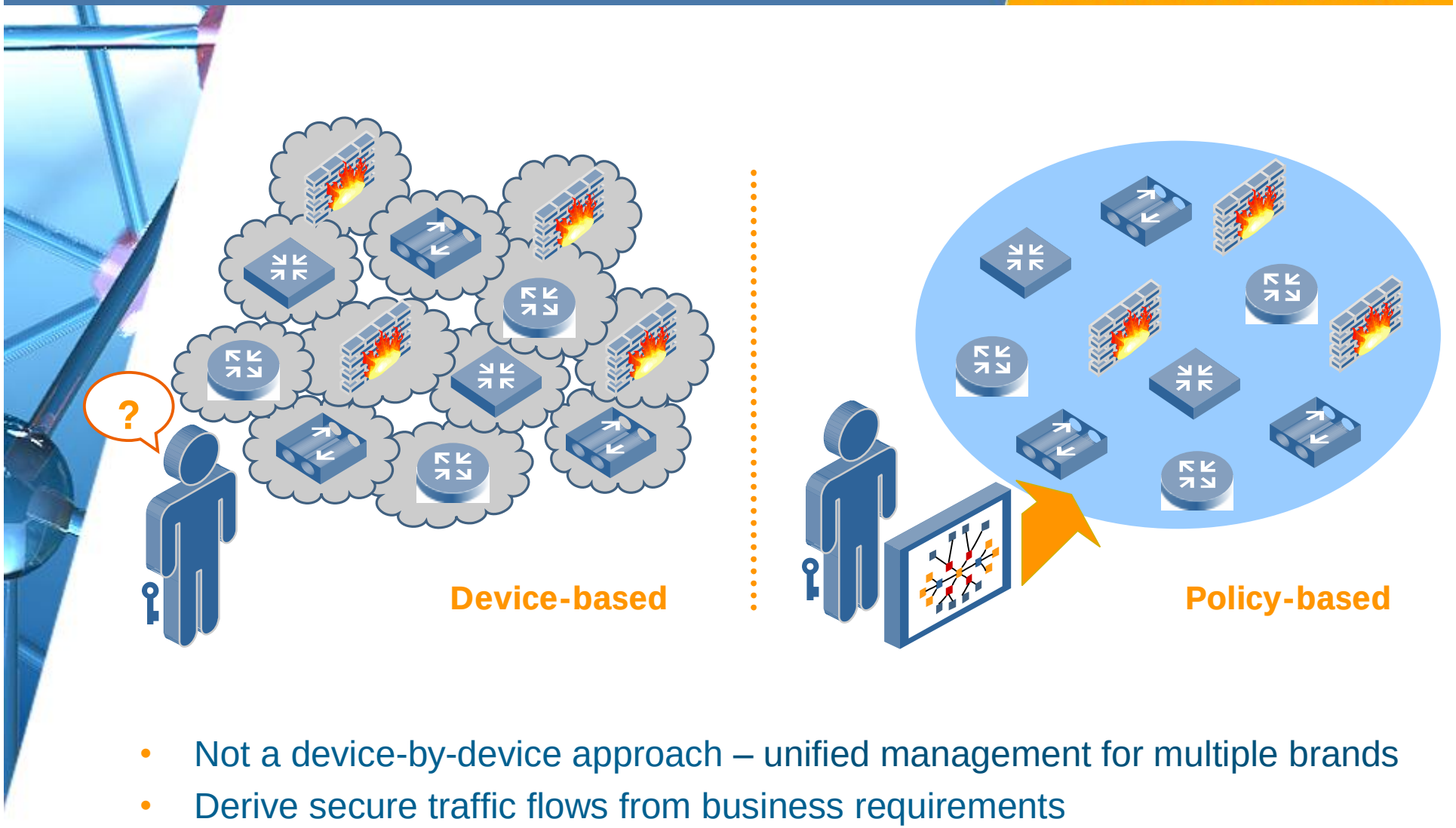
Complex device specific security rules

- **Access Control Lists**
- **Network Address Translation**
- **Anti-spoofing**
- **VPN IPsec (including DMVPN)**
- **Clusters and virtual systems**
- **Large VPNs**

Policy-Based Management

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

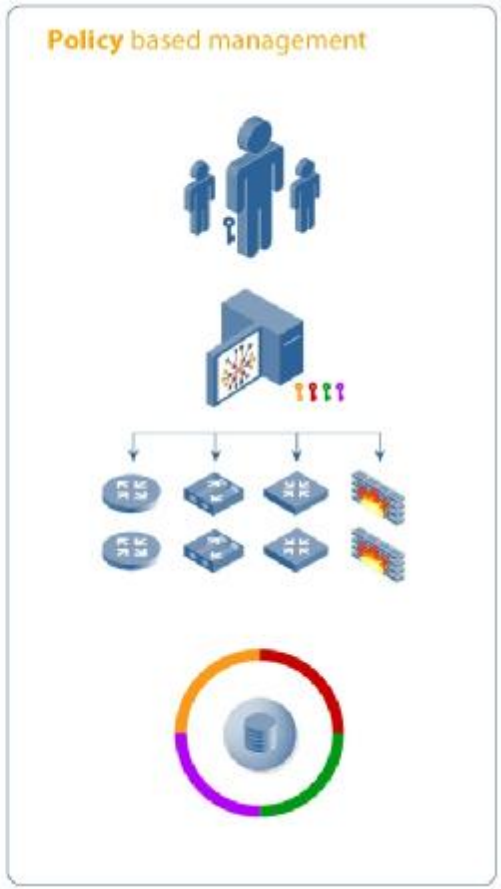


- Not a device-by-device approach – unified management for multiple brands
- Derive secure traffic flows from business requirements
- Consistent security policy across different types of devices

Policy-Based Management

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

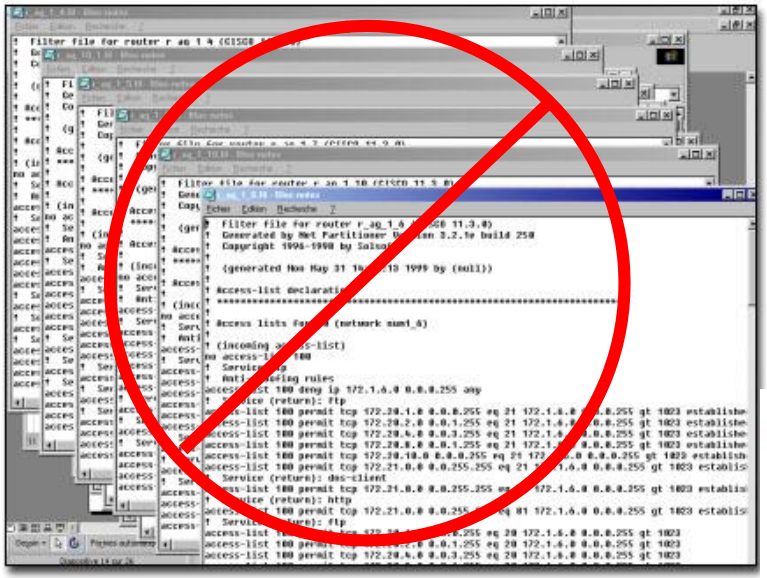


- Not a device-by-device approach – unified management for multiple brands
- Derive secure traffic flows from business requirements
- Consistent security policy across different types of devices

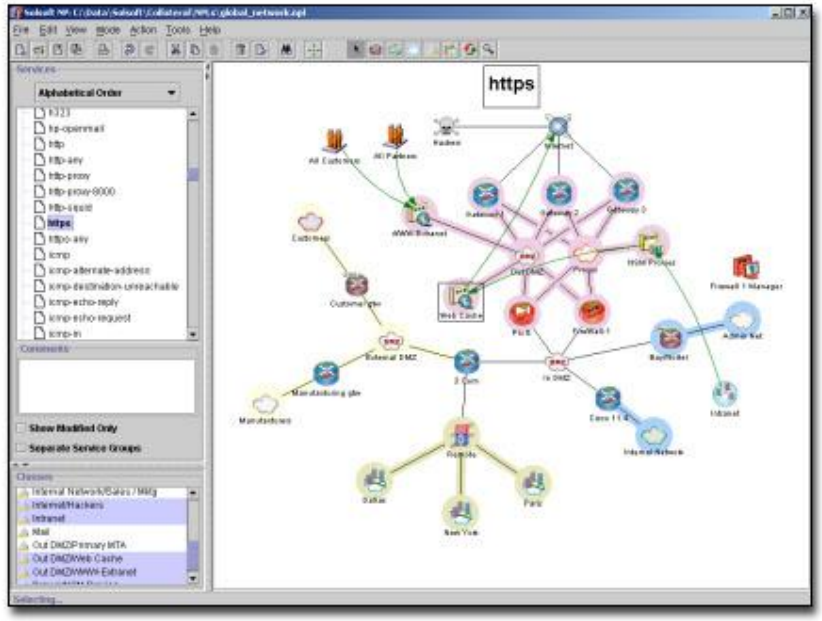
No Manual Coding

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



- Firewall Rules
- Access Control Lists
- Network Address Translation
- Anti-spoofing
- VPN IPsec
- Etc…



Divergence problem in manual approach

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Divergence problem explanation

SOLSOFT

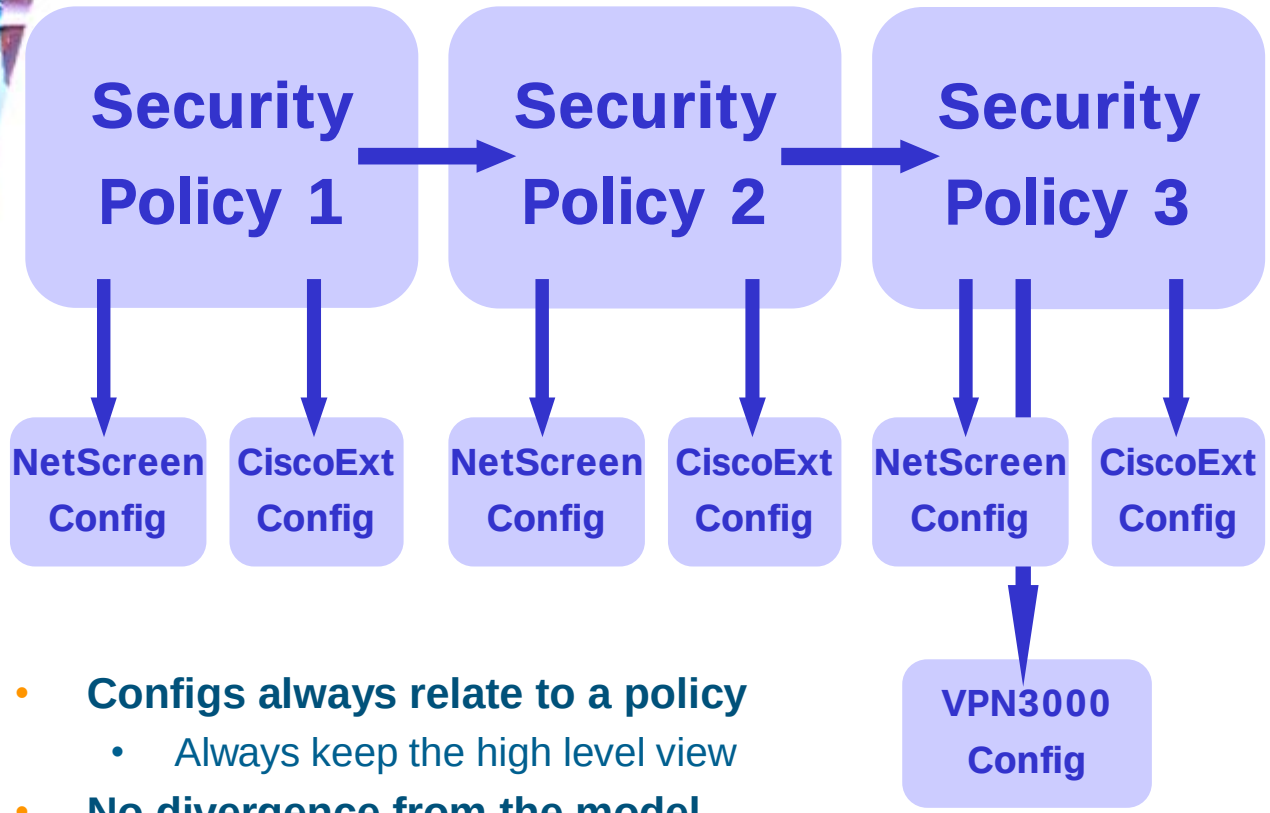
HOW SECURE NETWORKS ARE MANAGED

- **Configuration diverge from original policy model**
  - Business needs
  - Evolution over time
  - Hard to track why and who did the change
- **Problem is worse with increasing size**
  - Size double, complexity quadruple
  - Hard to communicate rationale behind changes, worse when bigger
- **Problem is worse with remote sites**
  - Remote sites make it even harder to communicate rationale
  - Different teams with overlapping territories

Solsoft solution to the divergence problem

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

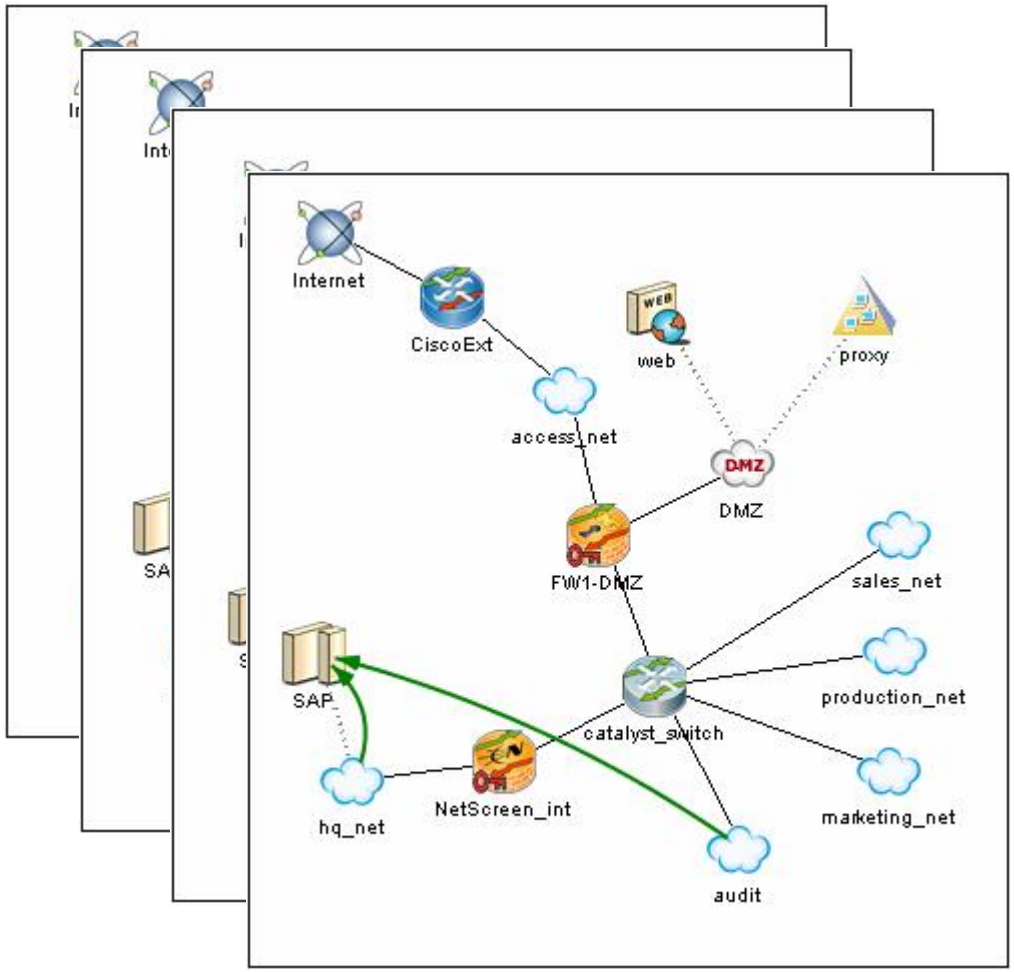


- **Configs always relate to a policy**
  - Always keep the high level view
- **No divergence from the model**
  - Everything inherits from model
- **Keep track of evolutions centrally**
  - Better than configuration management without model
- **Simulates impact**
  - Make informed decision.

Solsoft: Evolution without divergence

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



New permissions.

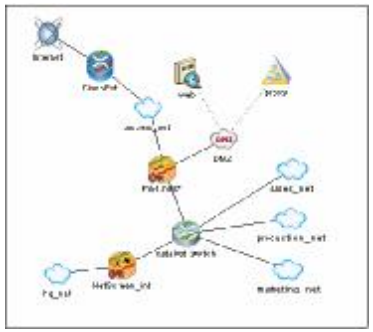
Solsoft: Evolution without divergence

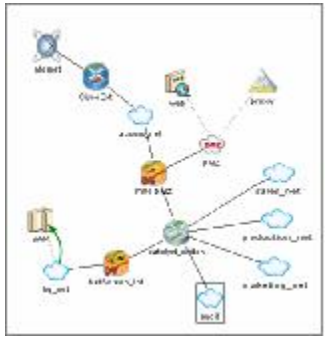
SOLSOFT

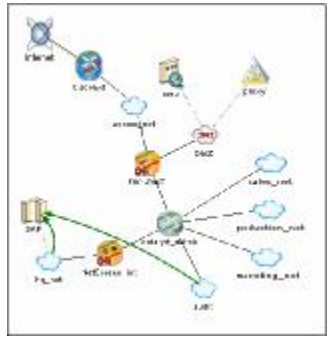
HOW SECURE NETWORKS ARE MANAGED

- Clearly visible evolution
- No divergence between policy and configurations
- All devices are in sync to fight the attackers with coherent ACLs
- Change management & Collaboration

Security Policy 1 → **Security Policy 2** → **Security Policy 3** → **Security Policy 4**





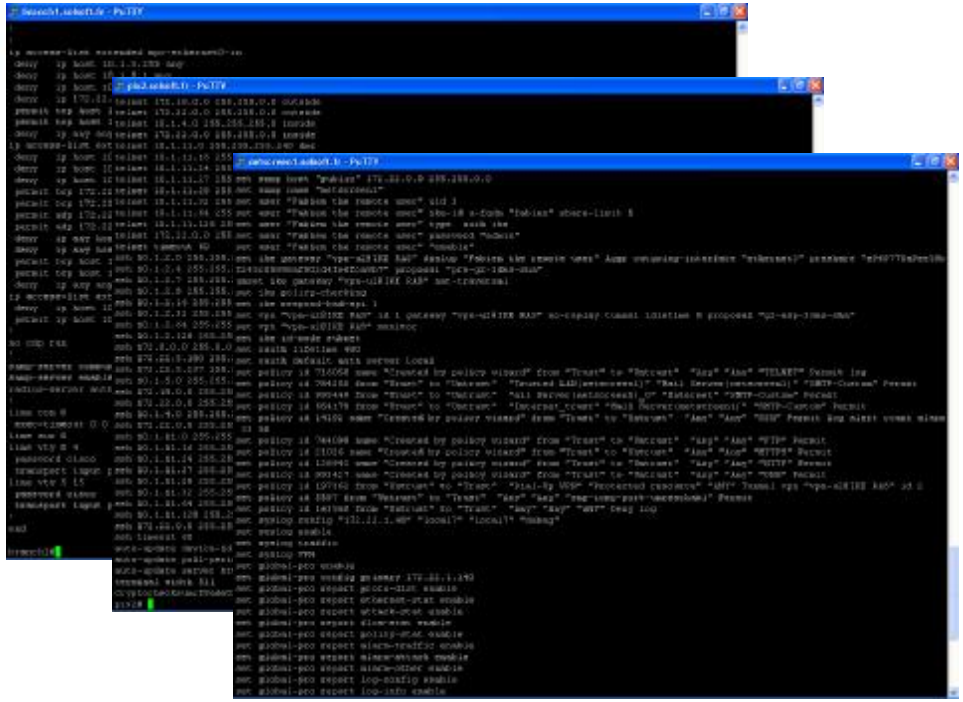


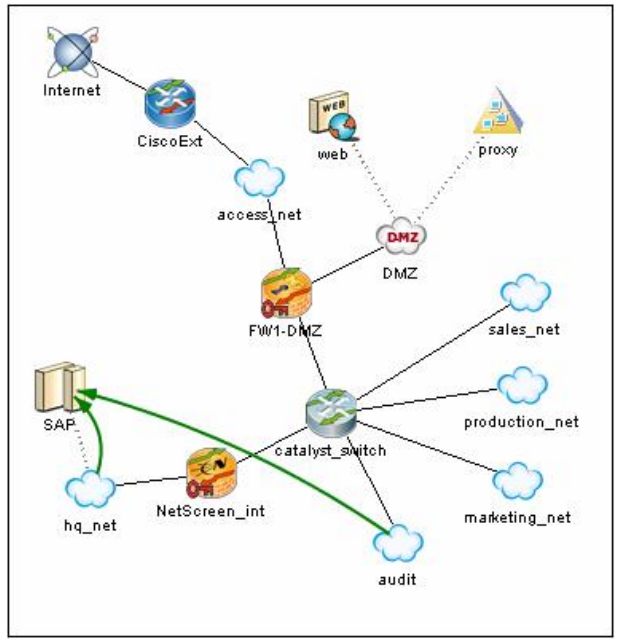
And it's better for auditing & searching

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

A picture is worth a thousand words!

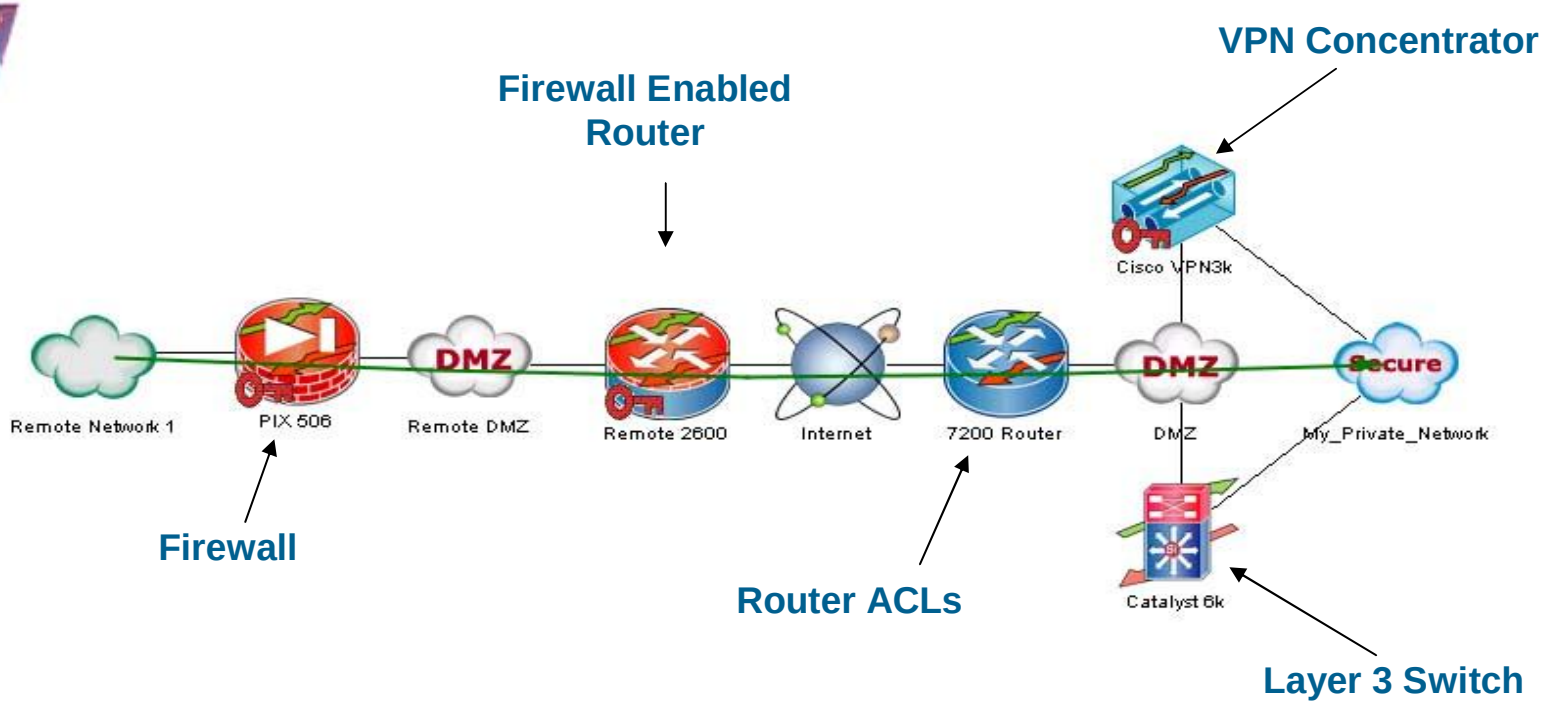




Consistent Security

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



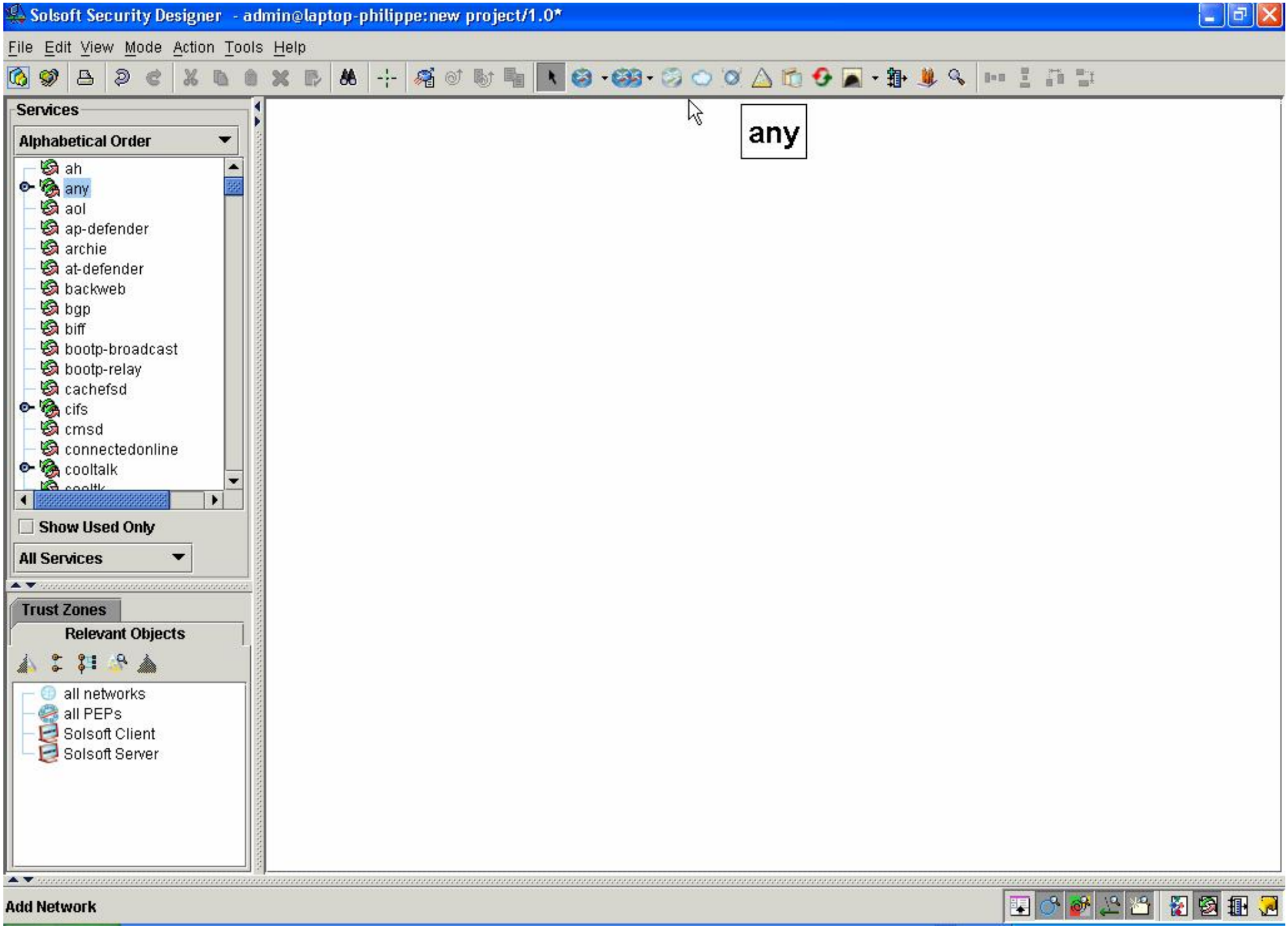
- "Topology aware" rule creation
- End-to-end rule enforcement
- "Deny All – Permit Some" principle

Solsoft Demonstration

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

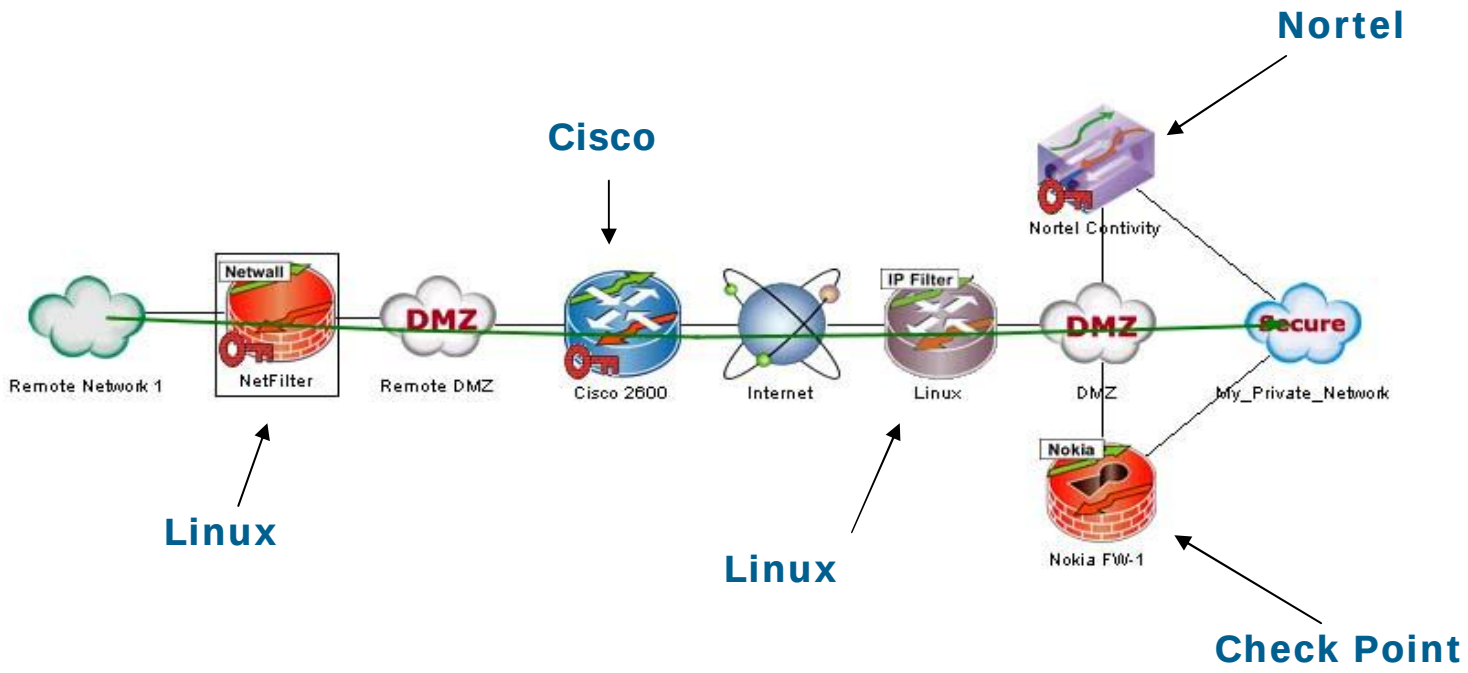
- Demo of Solsoft to build a policy map of a simple network


Solsoft Security Designer - admin@laptop-philippe:new project/1.0*
File Edit View Mode Action Tools Help
Services
Alphabetical Order
ah
any
aol
ap-defender
archie
at-defender
backweb
bgp
biff
bootp-broadcast
bootp-relay
cachefsd
cifs
cmsd
connectedonline
cooltalk
Show Used Only
All Services
Trust Zones
Relevant Objects
all networks
all PEPs
Solsoft Client
Solsoft Server
any
Add Network

Device Independence

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

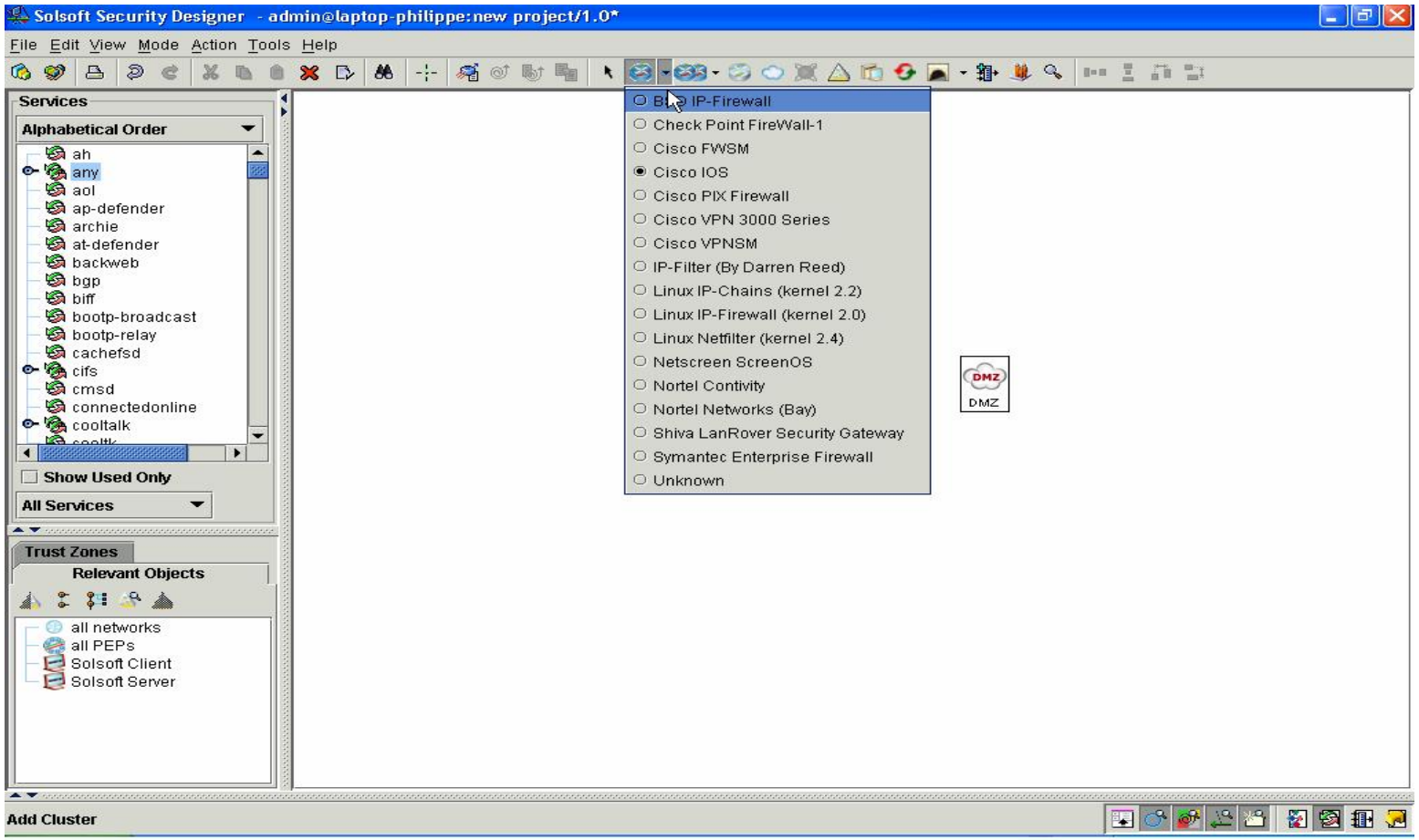


You draw arrows, no matter what kind of device it goes through!

Multi-vendor

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Place your routers and firewalls, transform a Cisco into a NetScreen

Device Security Profiles

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

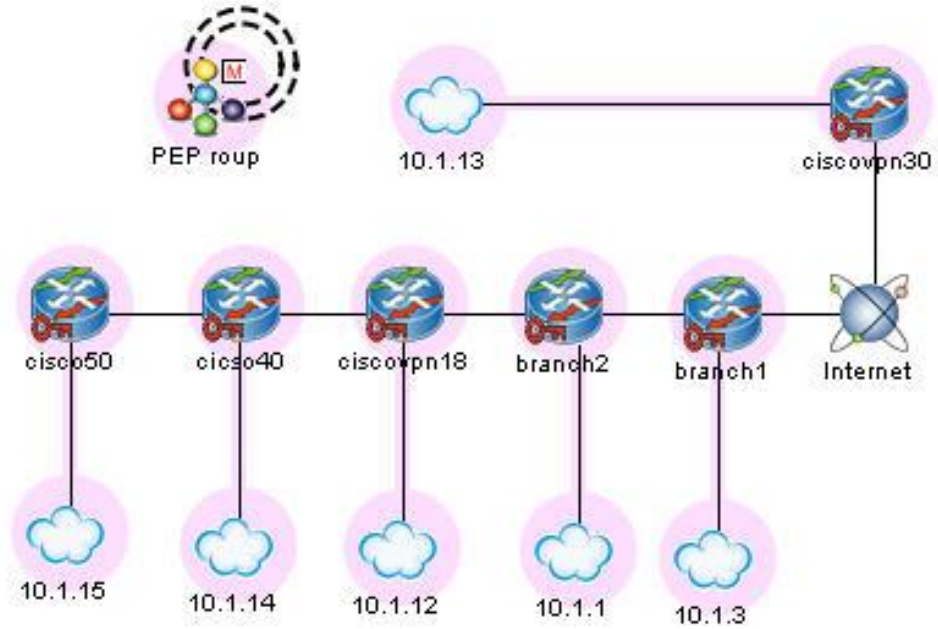
- **4 types of Device profiles**
  - No Filtering (Anti-spoofing only)
  - PEP Access security ((Anti-spoofing + PEP Access)
  - Low granularity (Optimized for reduced filter size on internal backbones)
  - Custom Filtering
- **Reduces filter size**
- **Simple setting for default behavior**
- **Devices are configured for a specific purpose**
  - Specialize device behavior
  - Avoid over-granularity in configuration
- **Optimization through policy**
  - Optimize easily the device configuration through policy settings and not manually set

VPN Tunnel Grouping

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Very simple visual design of VPN**
  - Setting a Fully meshed or Hub and Spoke is done in minutes
  - Optimized tunnel configurations are automatically calculated and configured
  - Supports heterogeneity and advanced features such as DMVPN



Fully meshed VPN with 6 devices, 6x5/2=15 tunnels

Immediate Policy Change

SOLSOFT

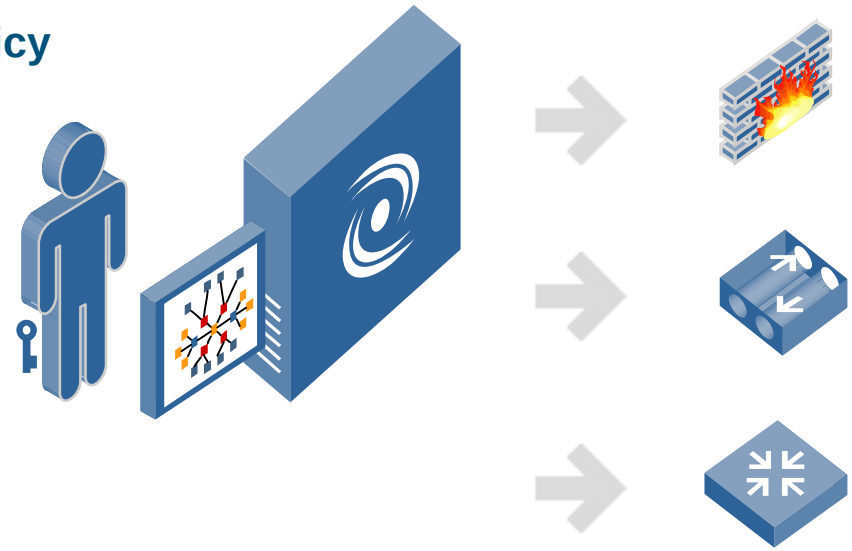
HOW SECURE NETWORKS ARE MANAGED

Rule Change

- Simple update
- Automatic calculation of new policy

Upload

- Secure communication
- Failsafe
- Rollback
- Device group ordering
- Progress reporting and logging

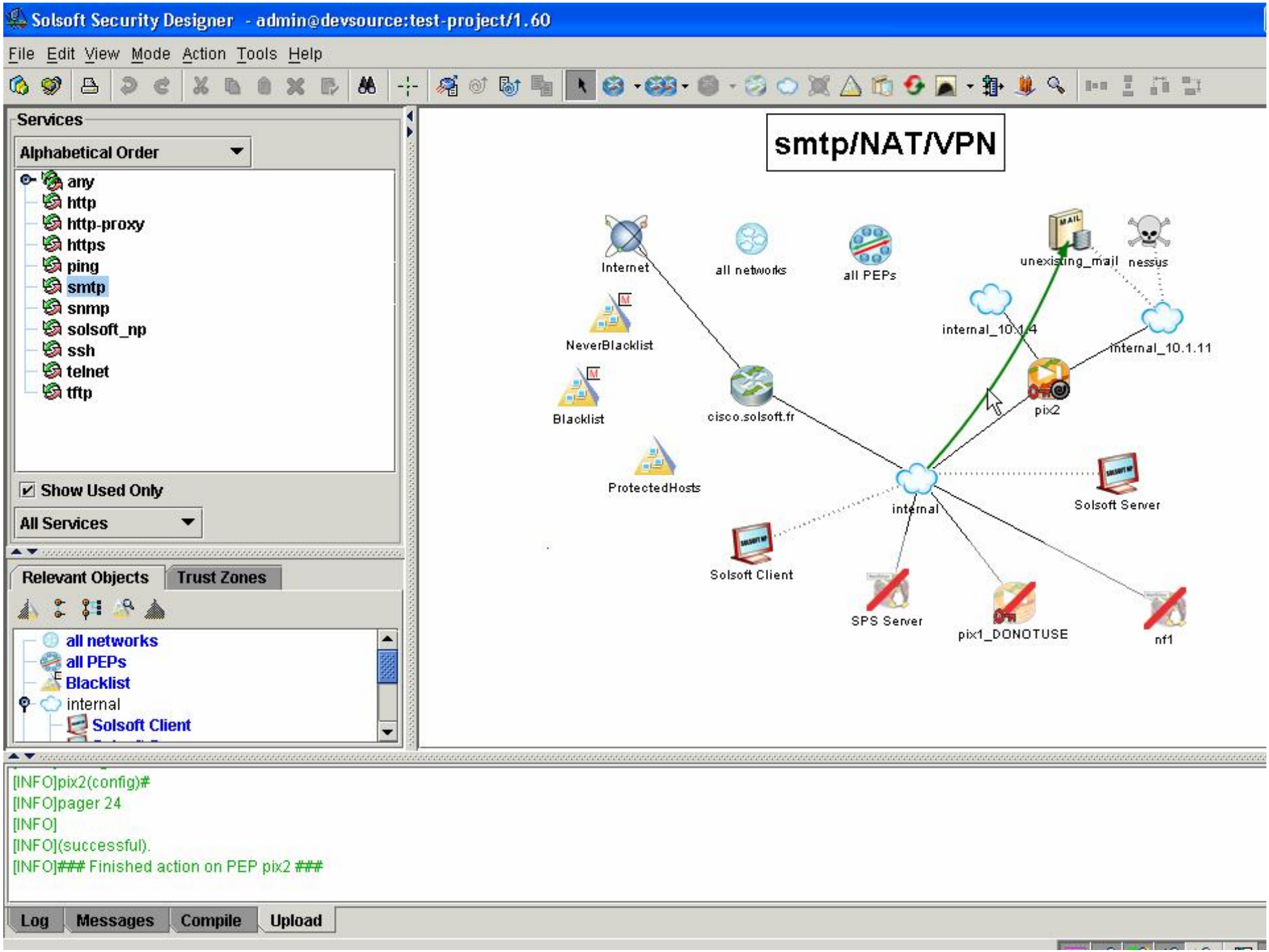


Upload demonstration

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

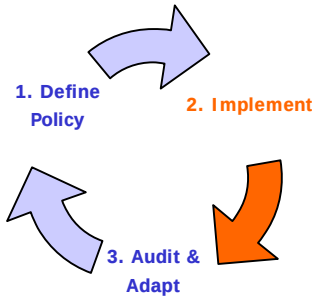
- **Video clip of an Upload session**
- **Speed is the normal speed**
- **Upload process is SSH**
  - Secured protocol
  - Could be anything from TFTP to low – speed, low security telnet
- **Upload targets**
  - One or several, doesn’t matter
  - Mixed devices or single-brand, doesn’t matter


Solsoft Security Designer - admin@devsource:test-project/1.60
File Edit View Mode Action Tools Help
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
smtp/NAT/VPN
Internet
all networks
all PEPs
unexisting_mail
nessus
NeverBlacklist
internal_10.1.4
internal_10.1.11
Blacklist
cisco.solsoft.fr
pix2
ProtectedHosts
internal
Solsoft Server
Solsoft Client
SPS Server
pix1_DONOTUSE
nf1
[INFO]pix2(config)#
[INFO]pager 24
[INFO]
[INFO](successful).
[INFO]### Finished action on PEP pix2 ###
Log
Messages
Compile
Upload

Solsoft Benefits on Upload

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



- **Scales very well**
  - Upload to hundreds of devices
- **Risk free upload process**
  - Manual configuration and upload, an error-prone task
  - Limit downtime due to Human-error
- **Multi-vendor**
  - No device-specific learning & training
- **Remove valuable human resources from the burden of repetitive tasks**
  - The number of device doesn’t matter
  - The different kinds of device doesn’t matter
- **Defense in depth is sustainable**
  - With any number of device
  - At any depth
- **Rollback to a valid previous configuration**
  - Always possible
  - Safety net for security and network / IT

Veritas Software

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

VERITAS™

Challenge

- Required unified management for their worldwide Cisco security products deployment covering VPN 3000, IOS VPN, PIX FW/VPN 525
- They were not satisfied with current Cisco management solutions

Selection Criteria

- Required a scalable, easy-to-use network management solution that is reliable and can handle the complexity of their growing network

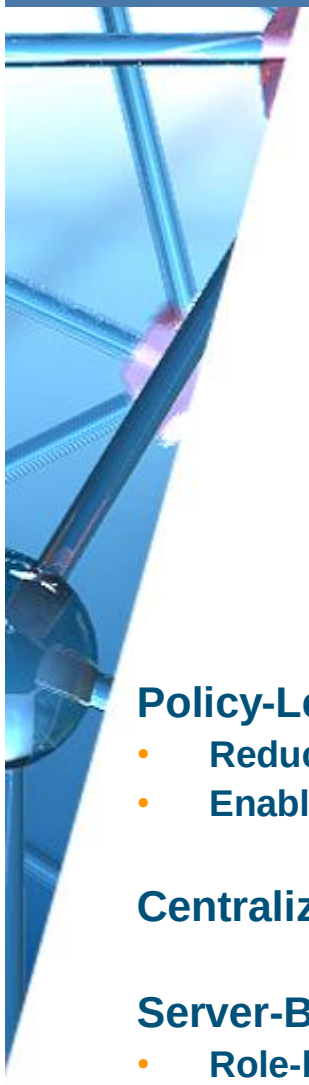
Solsoft Solution

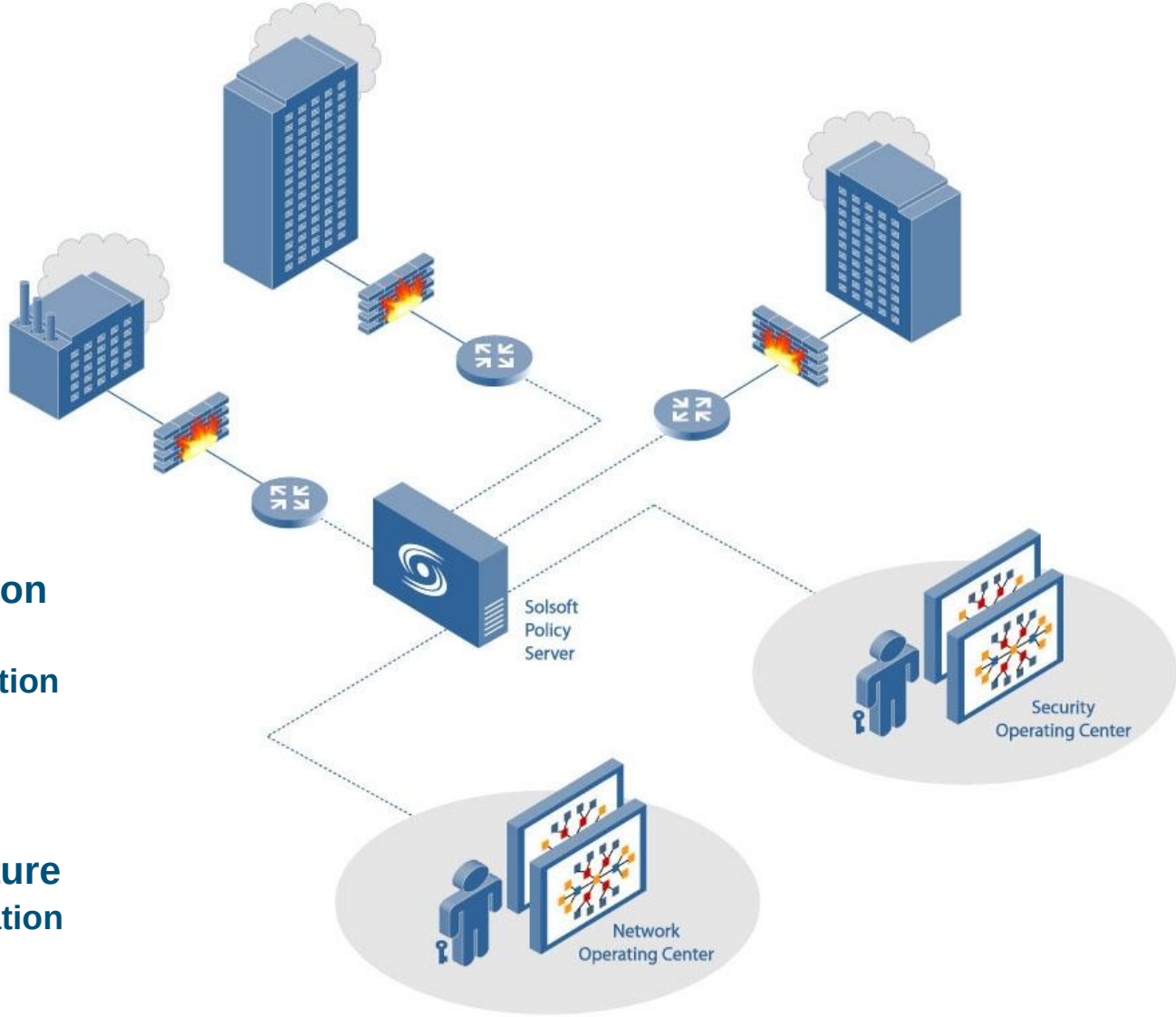
- "Compliance and preventive risk management is a paramount concern today. We standardized on the Solsoft Policy Server because it simplifies complex security and firewall configuration tasks and security policies. Our global security team takes advantage of Solsoft Policy Server's role-based management features to collaboratively manage our mission-critical firewall deployments."
  - Greg Valdez, CIO at VERITAS

Powerful Collaboration

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED





Policy-Level Visualization

- Reduces complexity
- Enables real collaboration

Centralized Repository

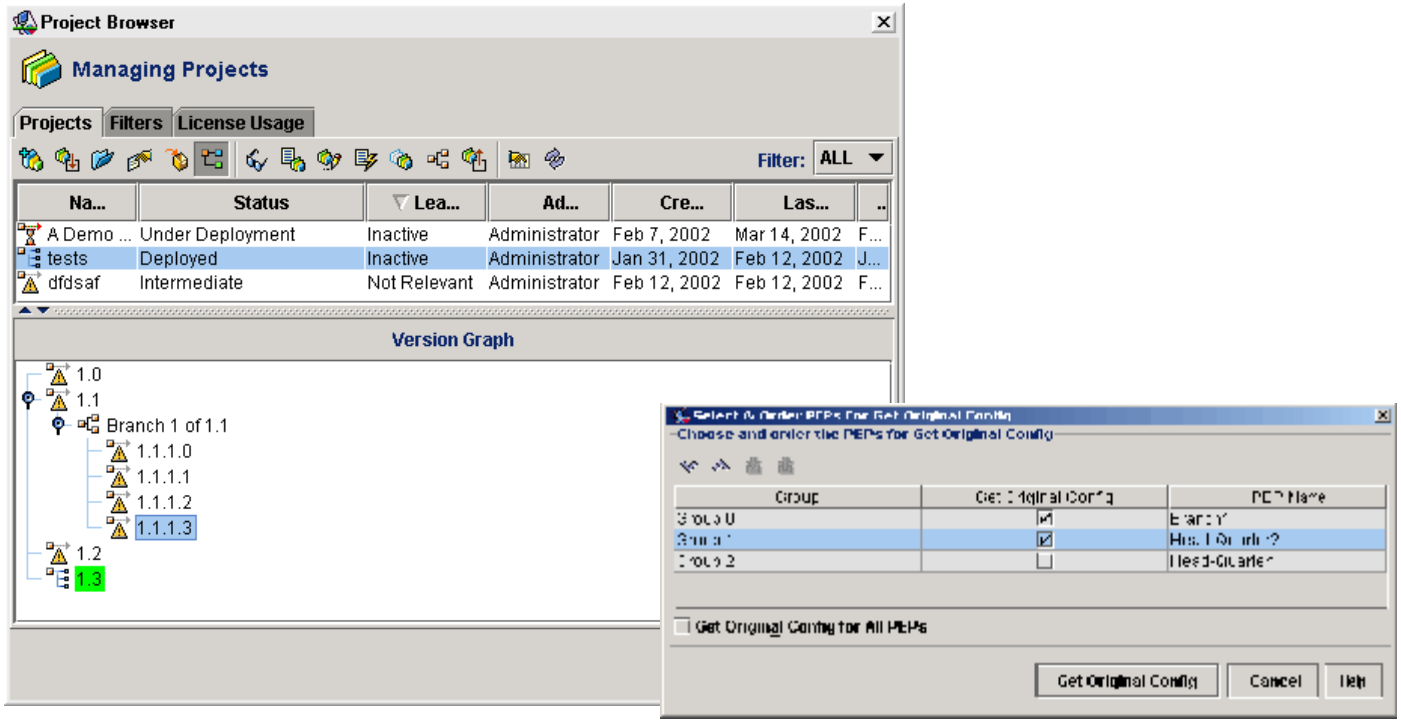
Server-Based Architecture

- Role-based administration
- Granular user profiles
- Project workflow

Policy Versioning

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



- Centralized policy repository
- All changes in policy are recorded
- Deployment and roll-back to ANY configuration at ANY time
- Expert scenarios can be designed and deployed as needed

Compliance Dashboard & Report Engine

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Web-based interface**
- **Network security dashboard**
  - Tabular rule view
  - Asset inventory
  - Deployment status
- **Query engine**
  - Canned & ad-hoc reports
  - Troubleshooting
  - Audits & change histories
- **Information sharing**
- **Schedule tasks**
- **Facilitates accountability and separation of duty**

Solsoft Security Reporter

SOLSOFT You are reviewing [Internet Gateways] version [1.3] Welcome [John C] Logout Administra

DASHBOARD | SECURITY POLICY | REPORTS | TASKS | Preference

Deployment | Assets | Rules | Search | Help

security policy > rules

Rules

save as repor

Search Results : **Criteria** Type : ALL Source: ALL Service : ALL Destination: ALL

Display : Object names, Object IP, Explicit Rules, Implicit Rules

New Search

sort by: Services go

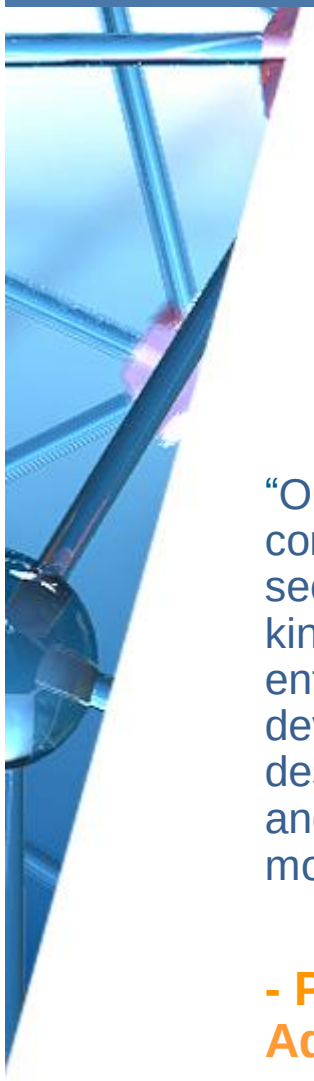
check all - clear all

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

Expert Opinion

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



META GROUP

“Organizations facing HIPAA, Sarbanes-Oxley, ISO, and other regulatory compliance challenges require practical and cost-effective solutions for network security intelligence and policy management. Solsoft's solution is the first of its kind to model the complex relationships between all network entities in an enterprise security topology, regardless of the brand or function of the security devices involved. The big win for compliance-savvy IT organizations is that design, deployment and auditing of network security policies - normally lengthy and labor-intensive undertakings - are now not only vastly easier, but also far more reliable."

- Paul Proctor, VP with META Group’s Security & Risk Strategies Advisory Service

Solsoft Technology Advances

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

	FEATURES	DEVICES	
2004	Web-based reporting VPN tunnel grouping Scheduling services Configuration optimization Reporting engine	Check Point NG AI Juniper Networks NetScreen 5 Nortel Networks Alteon Firewall Cisco VPN3000 4.1 Cisco FWSM 2.2	v6.0
2003	Virtual Systems support VPN Client to Gateway Web Services API PKI enablement Cluster management	Check Point NG Symantec EF Astaro Cisco Catalyst VPNSM NetScreen VPN	v5.3
2002	Server based architecture Multi-user management Role-based management Policy versioning	Nortel Networks Contivity Cisco PIX 6.x NetScreen Firewall Cisco Catalyst FWSM	v5.0
2001	Policy learning mode Firewall rule import Device SDK	NetFilter Cisco VPN3000 Intel NetStructure	v4.3
2000	IPsec VPN support Visual global NAT configuration	Check Point Firewall-1 4.x Cisco PIX 5.x	v4.0
1999	Support for Network Address Translation HP Open View Import	Cisco PIX Firewall 4.x Nortel Networks BayRS Cisco IOS Firewall, IOS 12.x	v3.2
1998	Visual interface representing Network Policy Policy audit by global analysis	StorageTek BorderGuard Bull NetWall 3.0	v3.0
1997	Network Policy Language Device configuration generator	Cisco IOS 9.21,10,11 IP Filter, IP Chains, IP Firewall	v2.0

Problem driven evolution

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

2002 **Compliance** → **Security Governance**

2000 **Adaptation** → **Manageability**

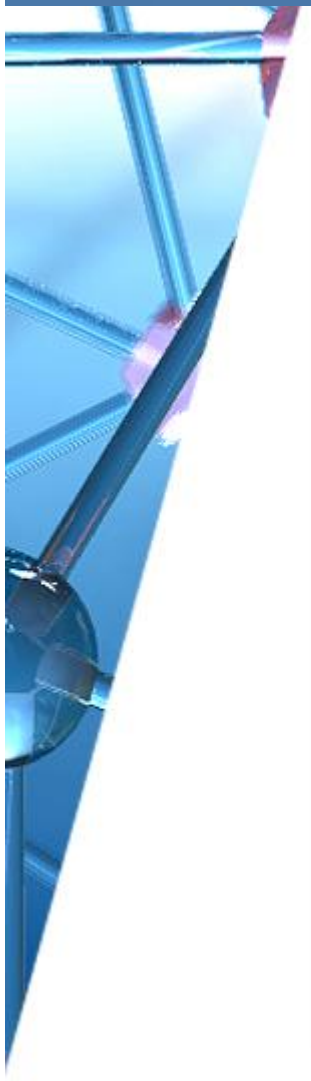
1997 **Implementation** → **Quality & Scalability**

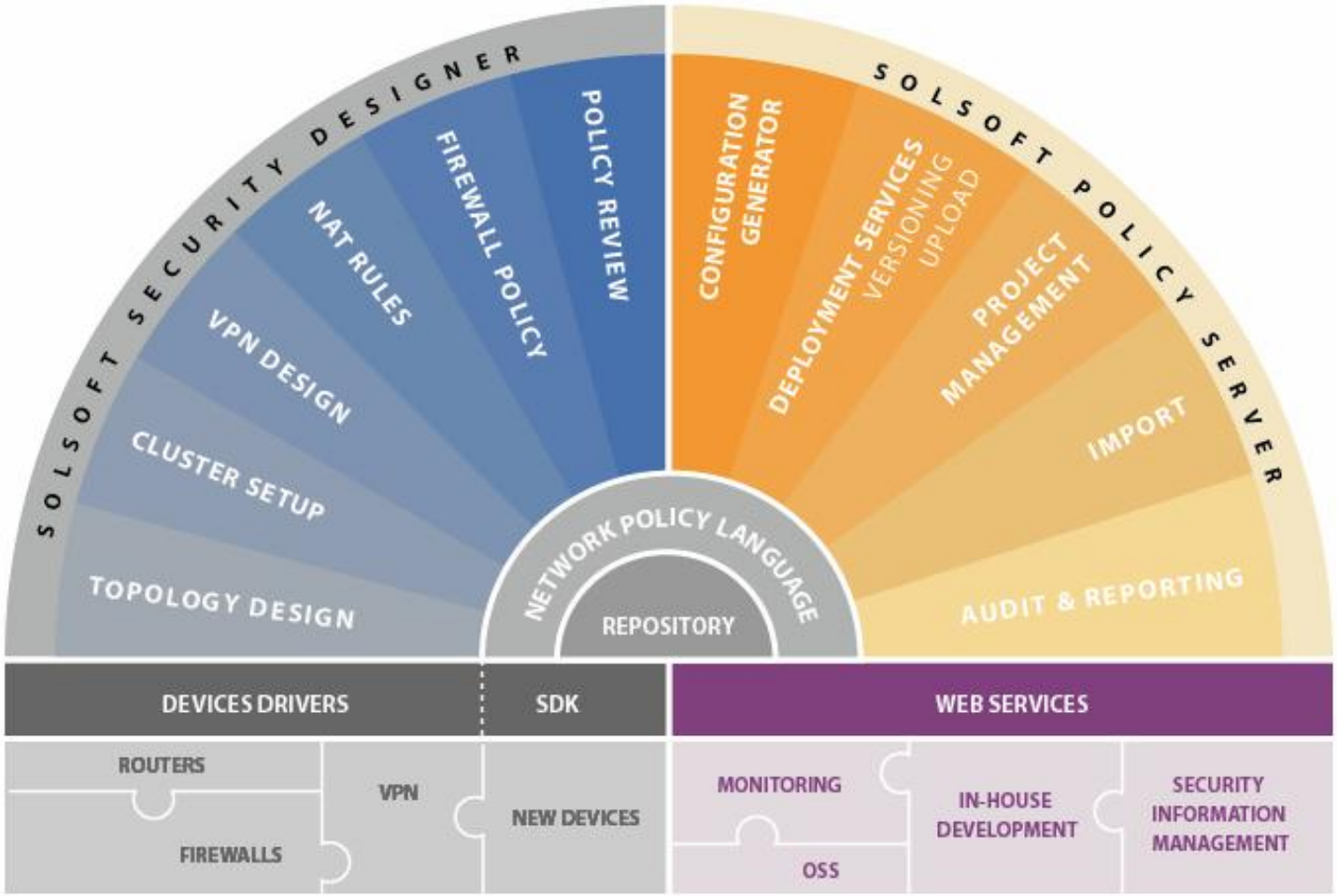
1994 **Design** → **Best Practices & Architectures**

Features Review

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED





Product Details

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

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.

Benefits Review

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Customer Benefits

- **Tighter Security**
  - Consistent security across the network with a common language
  - Fewer configuration errors and secure rule creation
  - Compliance with regulations (HIPAA, Sarbanes-Oxley, COBIT, GLB…)
- **Operational Solution**
  - Centralizes and automates policy creation and deployment
  - Enables teamwork and encourages process-driven culture
  - Instant and clear security review
- **Reduced Total Cost of Ownership**
  - Increases workforce efficiency and reduces training costs
  - Leverages existing equipment and provides future technology path
  - Lowers cost of device migration and vendor consolidation projects

Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- **Large Networks and Extremely Sensitive Networks**
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

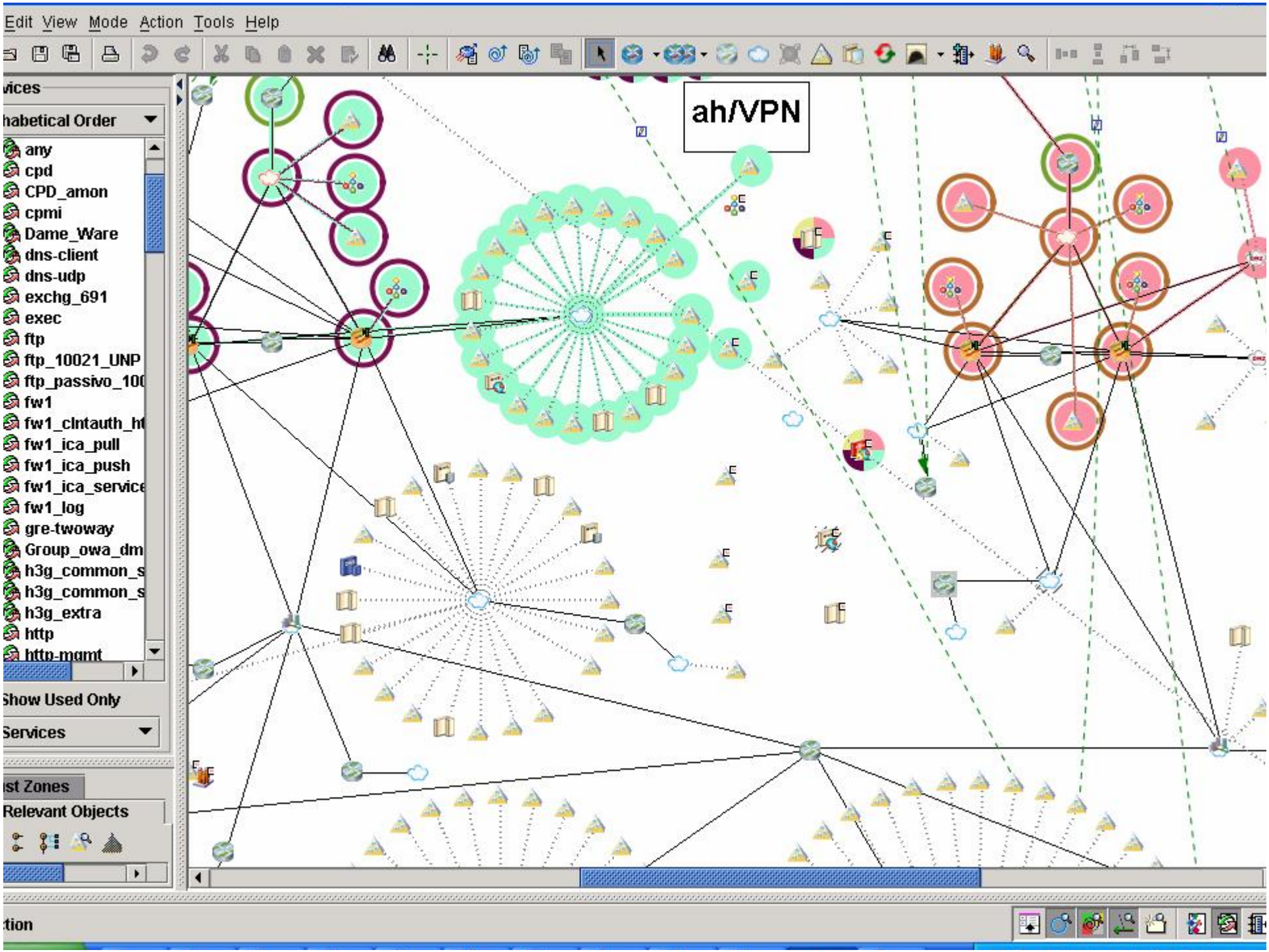
What is a large network

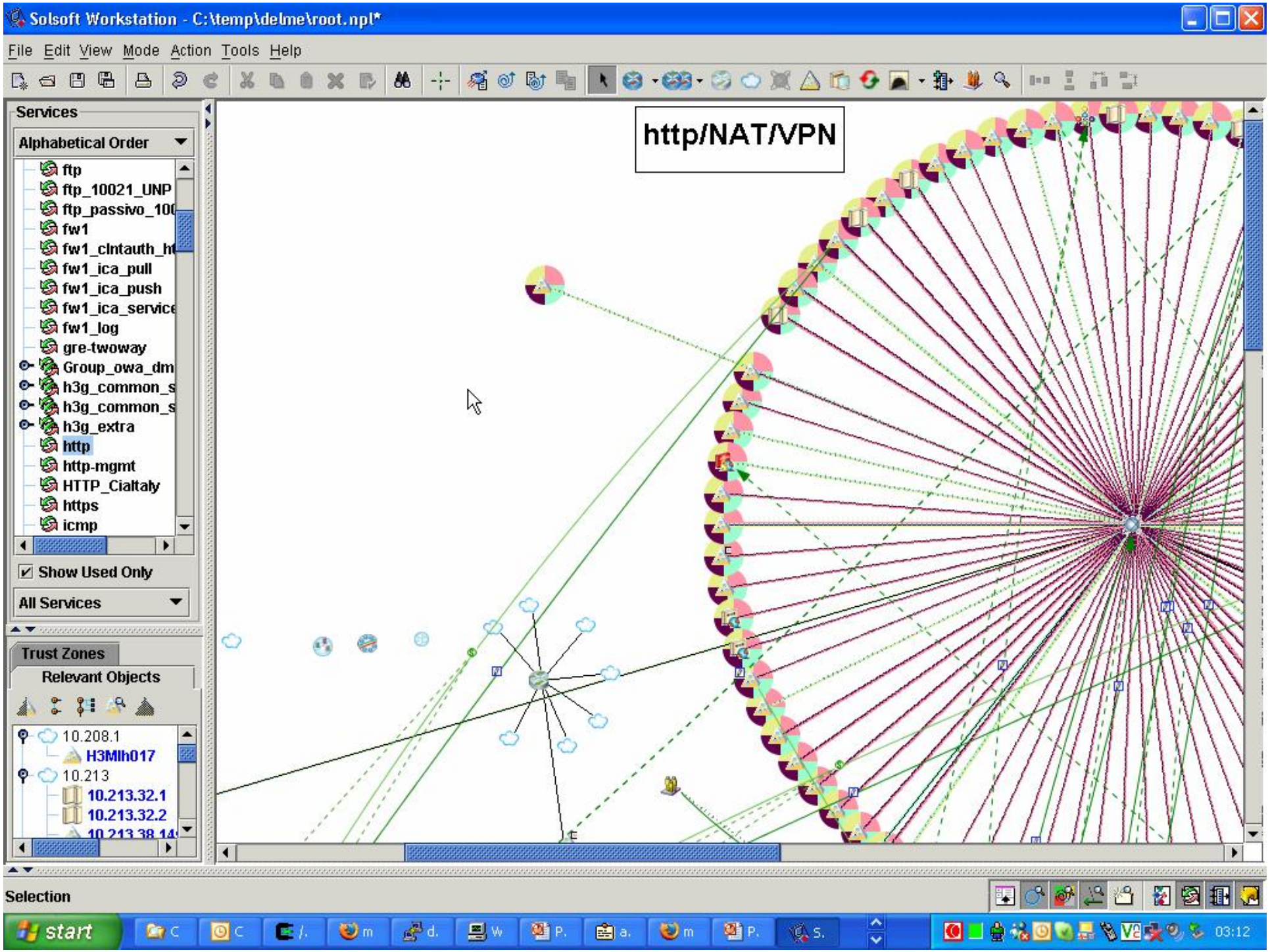
SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Thousands of hosts**
  - 5000 – 50,000
- **Hundreds of routers**
  - 100 – 800
- **Dozens of firewalls**
  - 15 – 70

- **What does it look like?**


Edit View Mode Action Tools Help
ah/VPN
any
cpd
CPD_amon
cpmi
Dame_Ware
dns-client
dns-udp
exchg_691
exec
ftp
ftp_10021_UNP
fw1
fw1_ica_pull
fw1_ica_push
fw1_log
gre-twoway
h3g_extra
http
Show Used Only
Services
Relevant Objects


Solsoft Workstation - C:\temp\delme\root.npl*
File Edit View Mode Action Tools Help
Services
Alphabetical Order
ftp
ftp_10021_UNP
ftp_passivo_10
fw1
fw1_clntauth_ht
fw1_ica_pull
fw1_ica_push
fw1_ica_service
fw1_log
gre-twoway
Group_owa_dm
h3g_common_s
h3g_common_s
h3g_extra
http
http-mgmt
HTTP_Cialtaly
https
icmp
Show Used Only
All Services
Trust Zones
Relevant Objects
10.208.1
H3MIh017
10.213
10.213.32.1
10.213.32.2
http/NAT/VPN
Selection
start
03:12

Wow!

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Ok, that makes Solsoft a tempting hack,**
  - but let’s work together instead! ;-)
- **Stats**

Risk, Vulnerabilities and Threats

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Risk = Vulnerability * Threat

- **For large networks**
  - Vulnerability = Number of exposed hosts * Average Vulnerability per host
  - What to do when number of exposed hosts is greater than 100?
  - When number of networks is greater than 500?
- **For extremely sensitive networks**
  - Threat is **high** because they are
    - Often attacked
    - Attacked by skilled hackers
- **Thus Risk is extremely HIGH!**

Where size and sensitivity matters…

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Best practices**
  - Deny by default on a large network is impossible when configured by hand
  - Thus forces trade-offs on internal security (usually)
- **Upload**
  - When you have to manually edit the configuration of 100 routers, you WILL do at least ONE mistake.
- **Automation**
  - Reactivity to attacks on large and extremely sensitive networks is extremely important
  - Usually, agencies and organization plan “lock down” configuration that are applied in case of big problem

Agenda

SOLSOFT

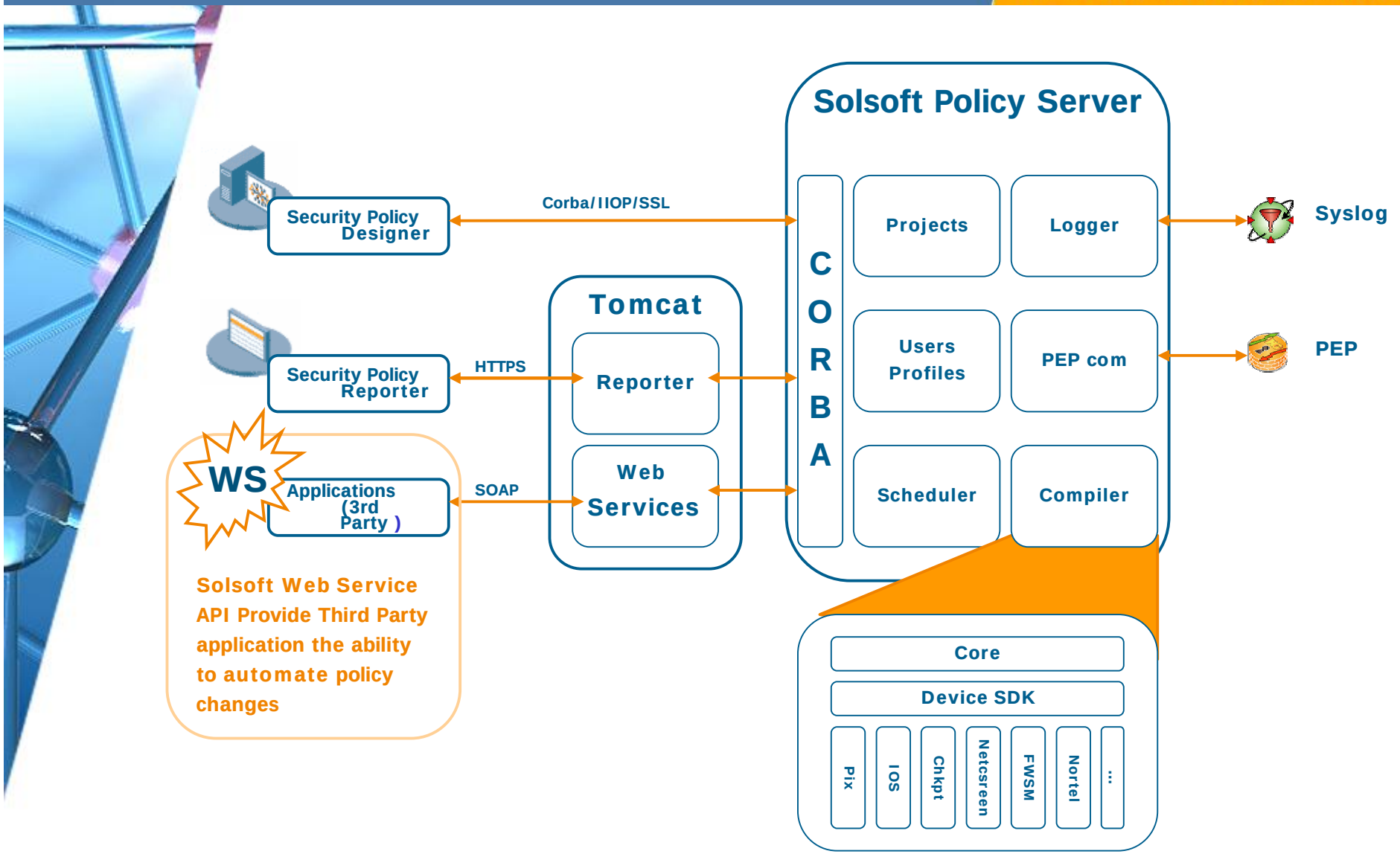
HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- **Open Architecture for Device Constructors: Device SDK**
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

Solsoft Architecture

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Multi-Vendor Interoperability

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Solsoft works with leading network security vendors to ensure constant interoperability**

- **Active support for :**
  - Cisco Systems
  - Check Point
  - Juniper/NetScreen
  - Nortel Networks
  - Symantec
  - Astaro
  - etc.

Cisco Systems AVVID Partner

Nortel Networks

symantec.

astaro internet security

Juniper Networks

Check Point Software Technologies Ltd.

Import and Migration

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Import firewall configurations from various vendors**
  - Objects
  - IP addresses
  - Security rules
- **From Cisco IOS configuration, PIX configuration, …**
- **Import configurations from HP OpenView**

HP OpenView PORTFOLIO PARTNER
HP OpenView CERTIFIED APPLICATION

- **Simple migration from one brand to another**
  - Change device properties of the object in Solsoft Security Designer
  - Configuration is automatically regenerated into the language of the target device
- **Switch from Cisco PIX to NetScreen**
  - It takes a click of the mouse and you can upload the new device.

Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- **Open Architecture for Security Software Companies: Web Service API**
- Advanced Open Source Projects
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

Dow Jones & Company

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

DOWJONES

Challenge

- Dow Jones wanted to consolidate their firewalls, utilizing a lower number of higher throughput devices.
- However, they needed a simple, scalable, centralized security management interface that supports NetScreen, Cisco PIX, Check Point FW-1 and Nortel Contivity

Selection Criteria

- Required a centralized, multi-vendor security policy management solution that was ***open*** and could grow with their business

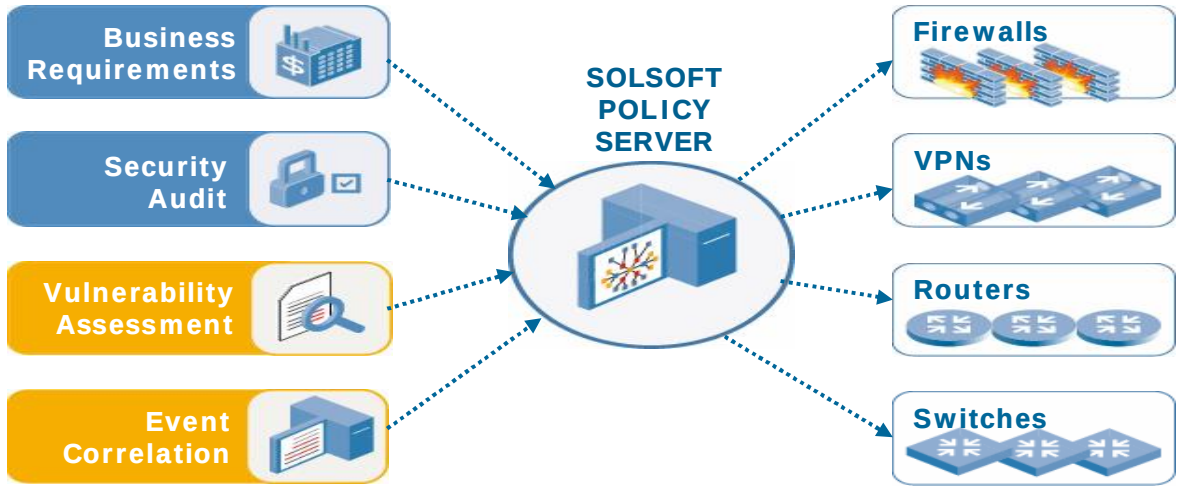
Solsoft Solution

- Dow Jones & Company chose Solsoft to configure and manage the firewall security infrastructure connecting all their business units and extranet customers.

Open Network Security Management

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



- **Solsoft Policy Server API**
  - 3rd-party products interoperability
    - Network monitors
    - Event Correlation / SIM
    - OSS
    - Help desk system
    - In-house and legacy applications
  - Web Services implementation

- **Solsoft Device SDK**
  - Productized SDK used internally
  - Built-in tools and training
  - Direct development support
  - Certification program
  - Short integration timeframe

Expert Opinion

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

DELPHI GROUP

"The next big step in the security marketplace will be to tie together Security Event Management (SEM) or Security Information Management (SIM) solutions with policy creation solutions, enabling rapid and coordinated reaction to policy violations. Solsoft is clearly positioned to take the lead in partnering with the wide variety of SIM/SEM solutions and significantly change the way security systems are handled, that is, systematically rather than millions of moving parts individually."

- Dan Keldsen, Senior Analyst, Consultant and Director of I.S. for Delphi Group

US ARMY SMS System CECOM

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Challenge

- Respond “on the fly” from a central location to intrusion detection alerts (ISS) and correlated events (Intellitactics)
- Unacceptable delay between detected attacks on Mobile Tactical Internet (Cisco routers and Symantec Raptor firewalls) and network operations response

Selection Criteria

- Required a fast, simple way to modify Access Control Lists (ACLs) and close down attacks

Solsoft Solution

- Solsoft provides automatic generation of ACL vs. manual coding
- Solsoft support for Symantec Raptor firewall provides US Army a central management solution for their Mobile Shelters’ Cisco 3600s, 7500s
- Intellitactics leverages Solsoft’s Web Services API for rapid reconfiguration
- Computer Science Corporation and large telco – systems integrators

Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- **Advanced Open Source Projects**
- The future: GRID, Reaction to worms, Global IPS, Global HoneyPot

What is it?

SOLSOFT

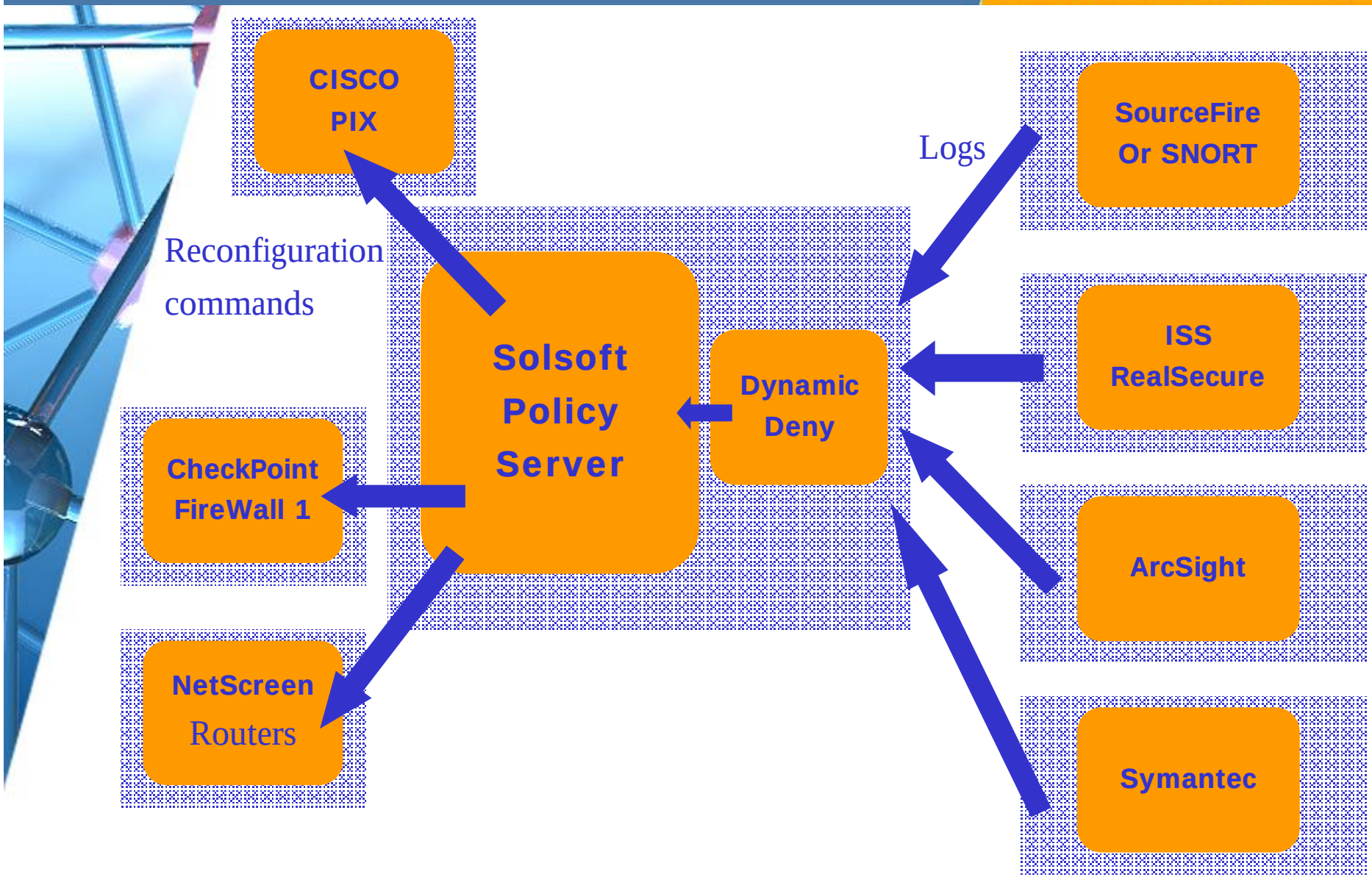
HOW SECURE NETWORKS ARE MANAGED

- Dynamic Deny is an example of integration of IDS with Solsoft Policy Server
- It blocks attackers IP addresses in firewall
- Using Web Services API
- A client Java program to call Web Service API
- A parsing script developed in Python to parse SNORT logs

Dynamic Deny Global Overview

SOLSOFT

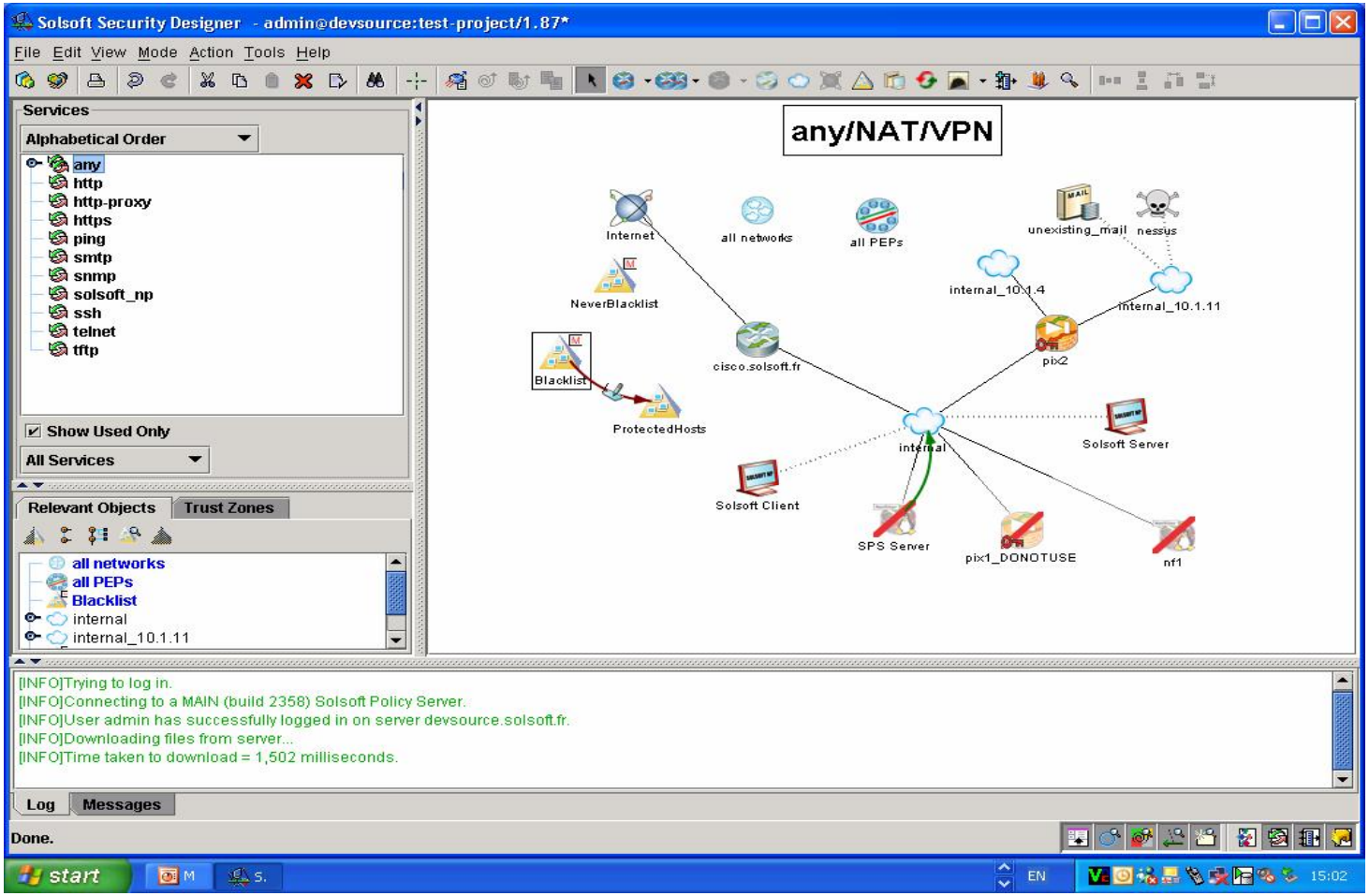
HOW SECURE NETWORKS ARE MANAGED



Test Project Map

SOLSOFT

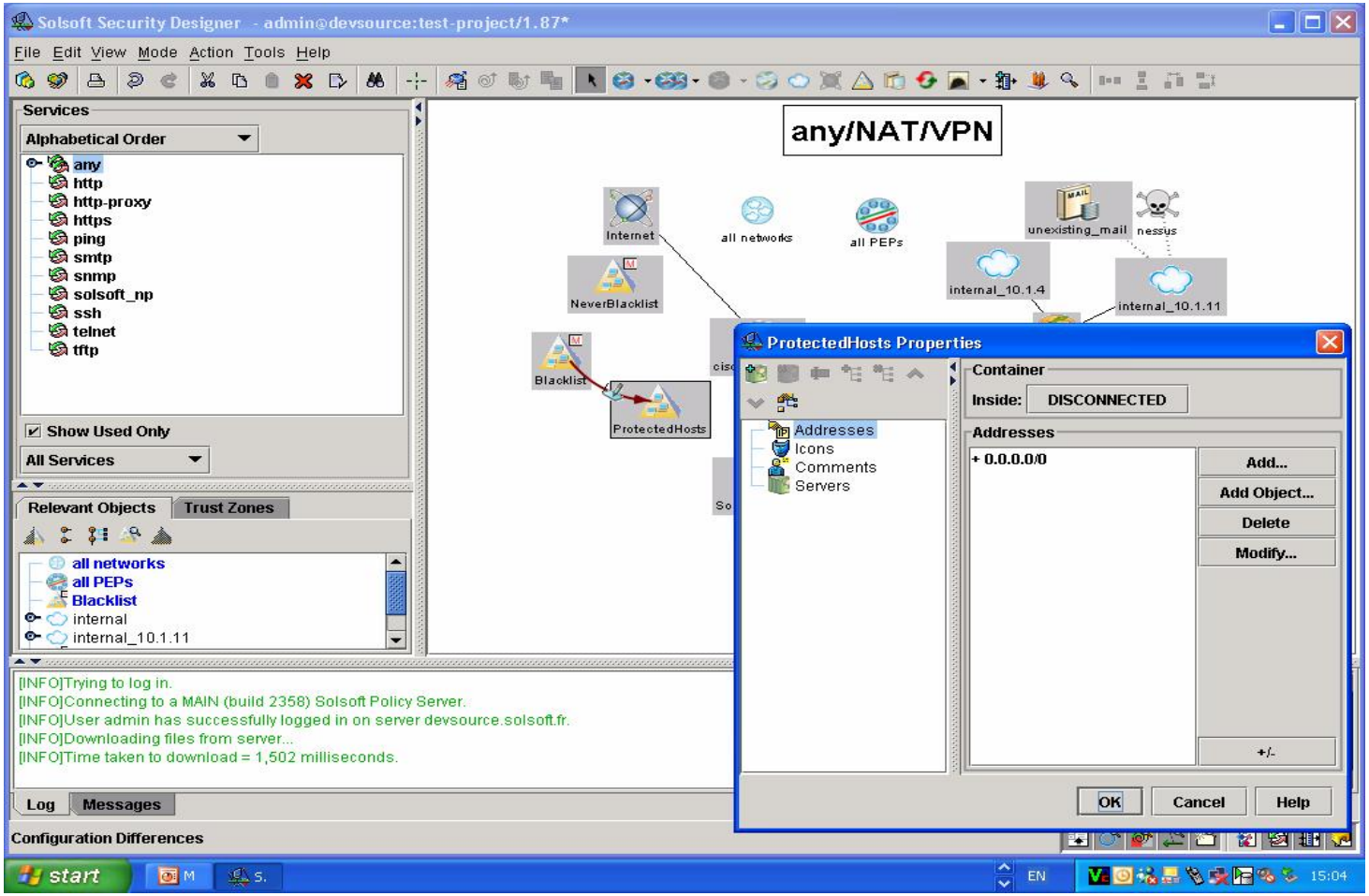
HOW SECURE NETWORKS ARE MANAGED



Protected Hosts

SOLSOFT

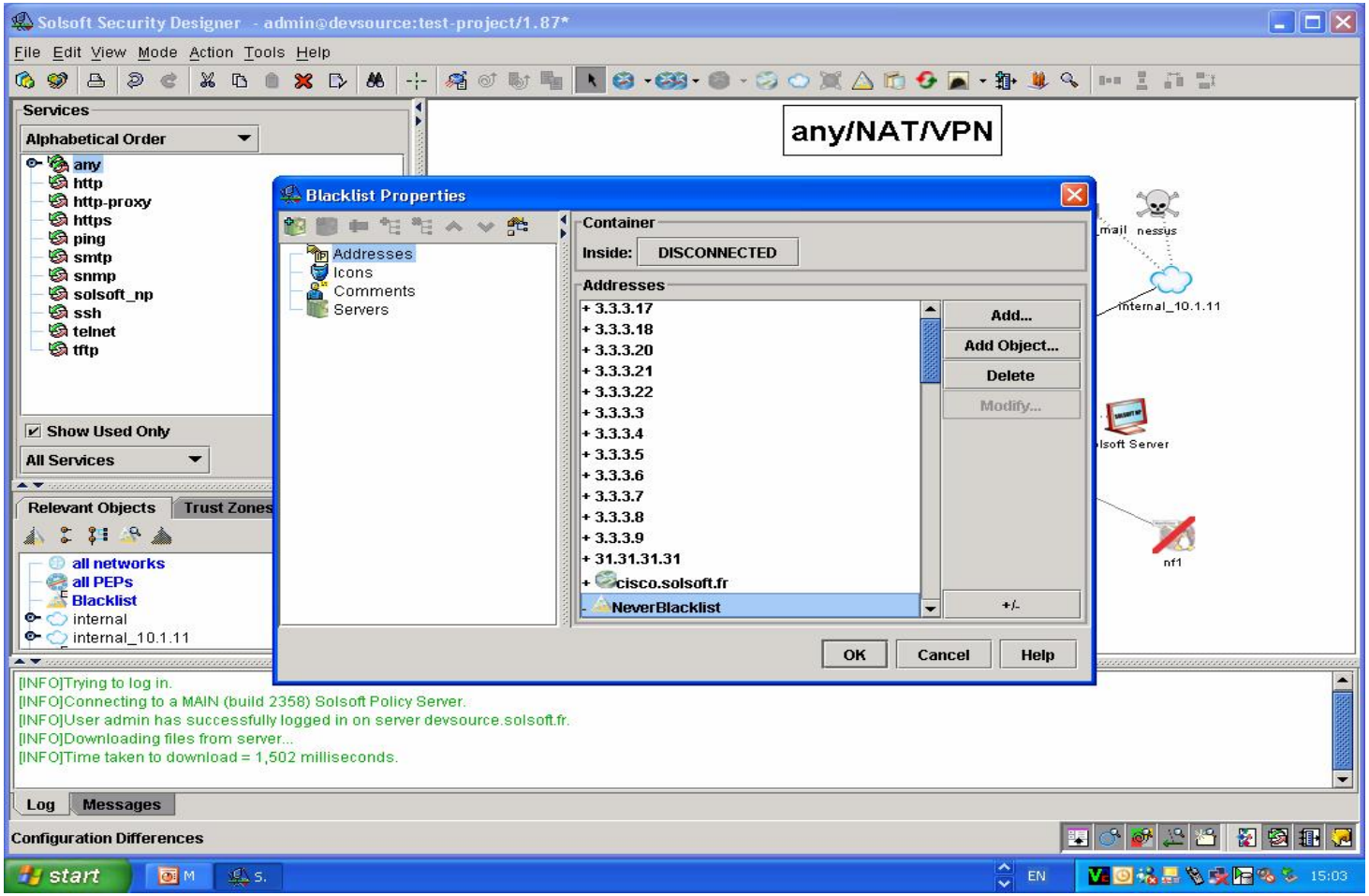
HOW SECURE NETWORKS ARE MANAGED



Substraction of classes

SOLSOFT

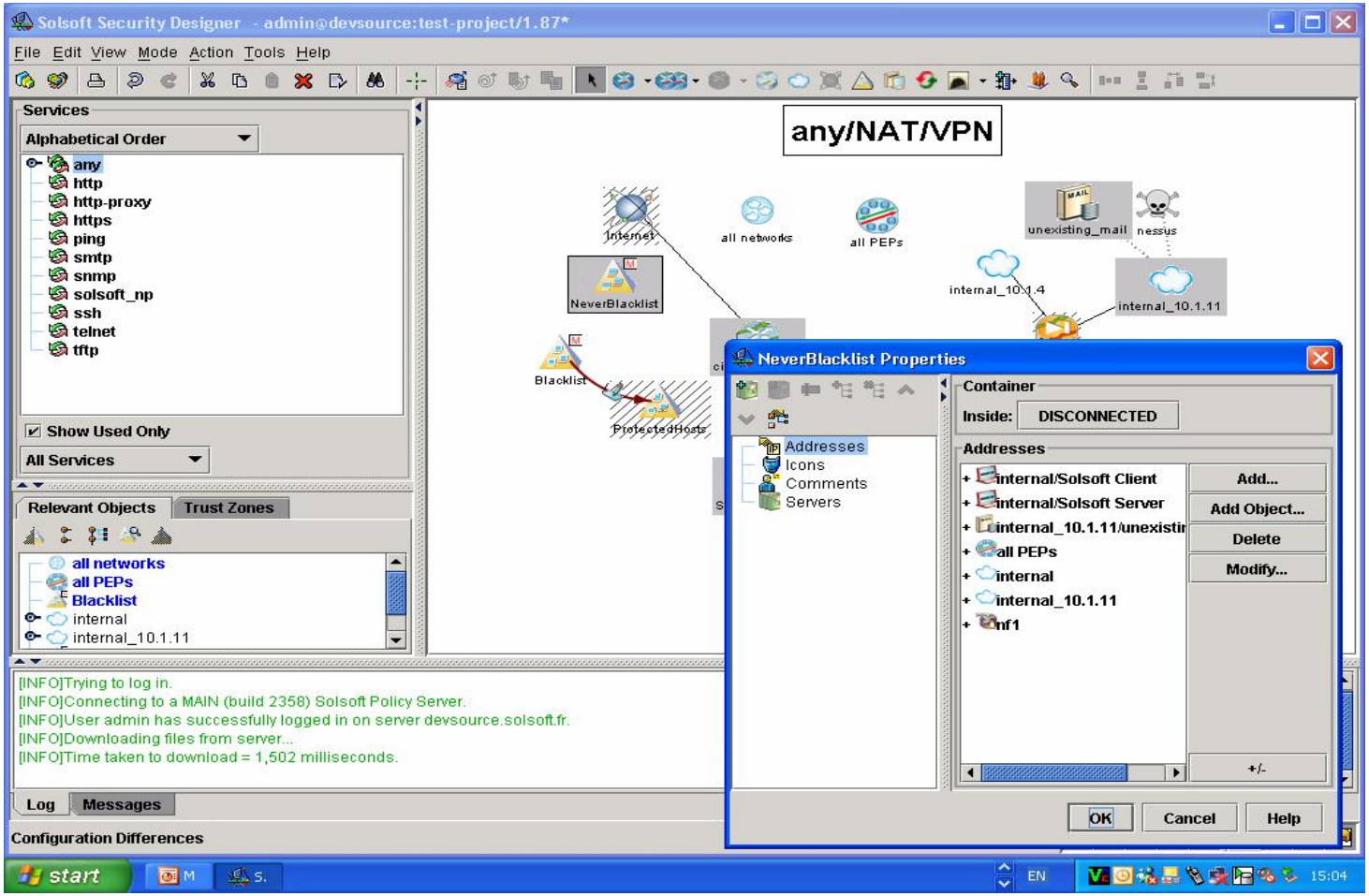
HOW SECURE NETWORKS ARE MANAGED



Substracted class

SOLSOFT

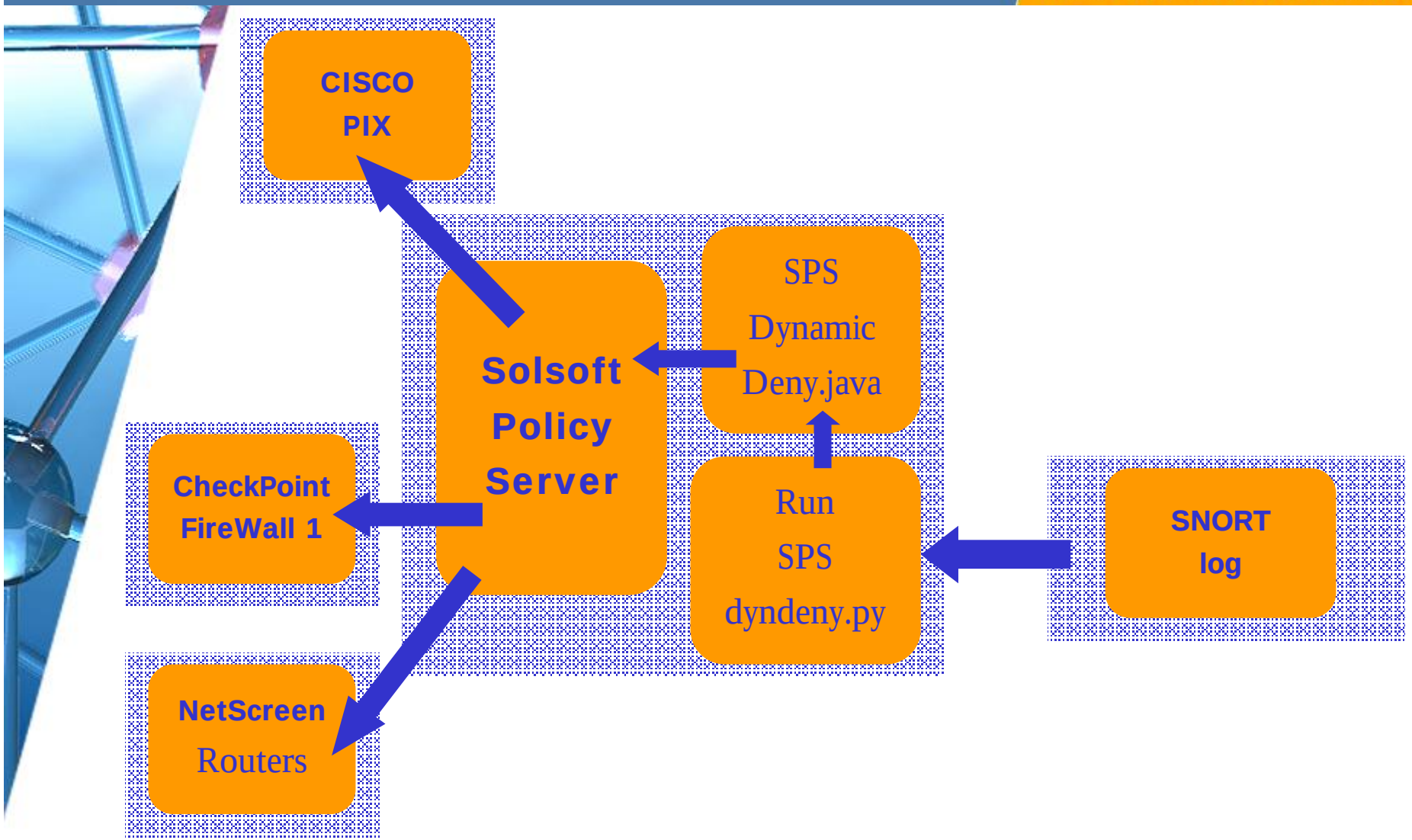
HOW SECURE NETWORKS ARE MANAGED



Dynamic Deny Internal Design

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

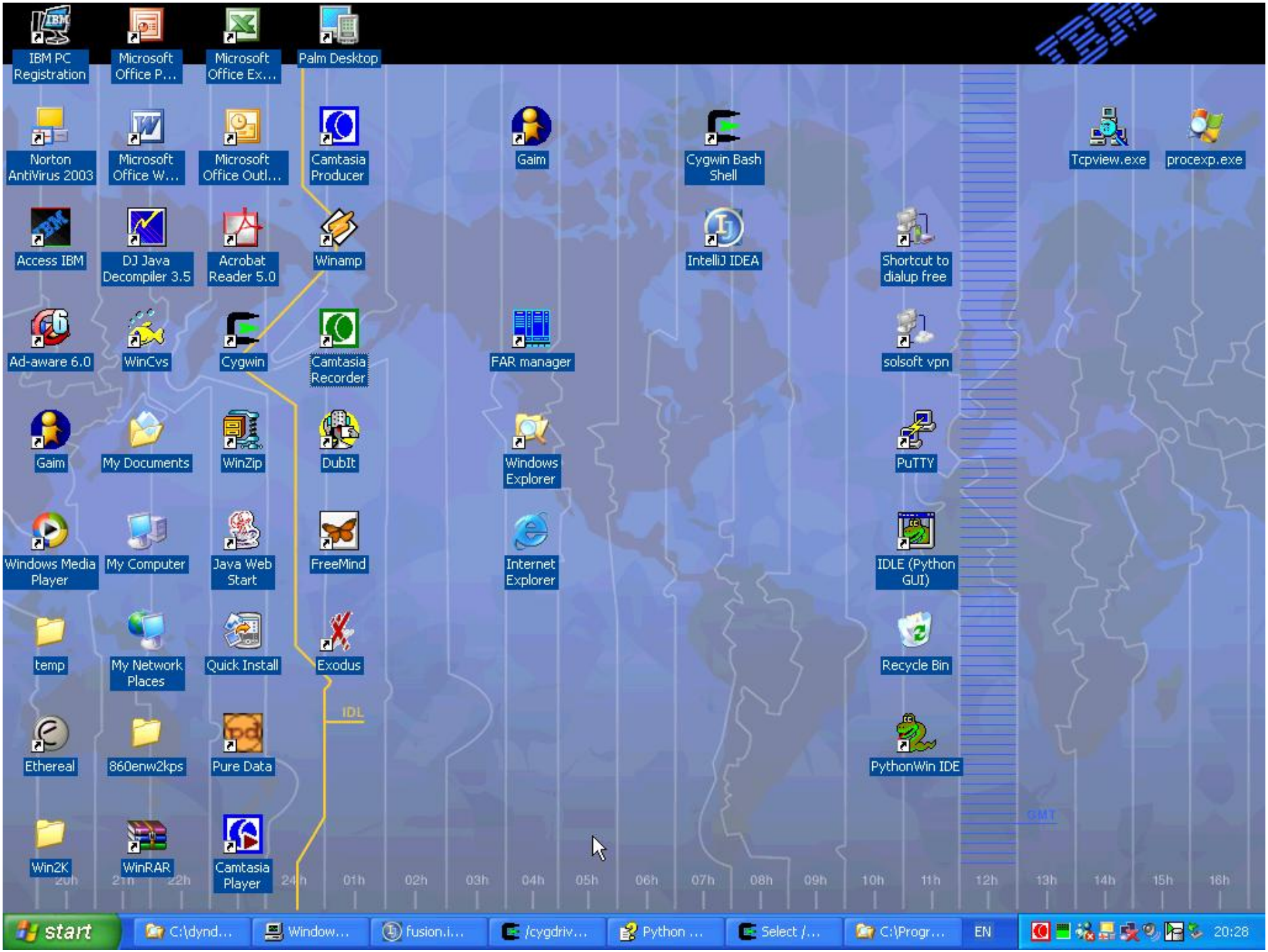


DynDeny Demonstration

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Following is a video record of a demonstration of DynDeny
- Integrated with SNORT
- Detecting a NMAP scan from another machine
- Blacklisting the attacker IP in the firewalls configurations


IBM PC Registration
Microsoft Office P...
Microsoft Office Ex...
Palm Desktop
Norton AntiVirus 2003
Microsoft Office W...
Microsoft Office Outl...
Camtasia Producer
Gaim
Cygwin Bash Shell
Tcpview.exe
procexp.exe
Access IBM
DJ Java Decompiler 3.5
Acrobat Reader 5.0
Winamp
IntelliJ IDEA
Shortcut to dialup free
Ad-aware 6.0
WinCvs
Cygwin
Camtasia Recorder
FAR manager
solsoft vpn
Gaim
My Documents
WinZip
DubIt
Windows Explorer
PuTTY
Windows Media Player
My Computer
Java Web Start
FreeMind
Internet Explorer
IDLE (Python GUI)
temp
My Network Places
Quick Install
Exodus
Recycle Bin
IDL
Ethereal
860enw2kps
Pure Data
PythonWin IDE
Win2K
WinRAR
Camtasia Player
GMT
20h
21h
22h
24h
01h
02h
03h
04h
05h
06h
07h
08h
09h
10h
11h
12h
13h
14h
15h
16h
start
C:\dynd...
Window...
fusion.i...
/cygdriv...
Python ...
Select /...
C:\Progr...
EN
20:28

Question & Answers

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **Blacklisting is dangerous, how do you prevent the good guys (i.e. my main server) from being blacklisted?**
  - Solsoft Policy Server provides this through the “NeverBlacklist” object.
  - It can be seen as a “white list”
- **I don’t use SNORT**
  - If you use something else, you can adapt easily dyndeny python script (mainly modifiying the libdyndeny.py file) to read other formats.
  - It’s easy to do so with text based (not binary) log files.

Agenda

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- Who is Solsoft?
- Security Context
- Solsoft Policy Server - Presentation and Demonstration
- Large Networks and Extremely Sensitive Networks
- Open Architecture for Device Constructors: Device SDK
- Open Architecture for Security Software Companies: Web Service API
- Advanced Open Source Projects
- **The future: GRID, Reaction to worms, Global IPS, Global HoneyPot**

Global HoneyPot

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

- **DynDeny is only an example, not a feature complete product**
- **Instead of denying, NAT the traffic from “blacklist” to a HoneyPot.**
  - When an attacker is detected, he is silently being NAT’ed into a HoneyPot box
  - Can watch attackers automatically coming to the HoneyPot
  - Securely from the Sebek box.
  - Detect intent.
- **You can make several improvements:**
  - Provide some statistics about blacklisting
  - Be more configurable through config file / property file usage
  - Support more IDS / Event Correlation log
    - Concurrent / parallel log file reading support is provided within the Python script.

GRID Network example

SOLSOFT

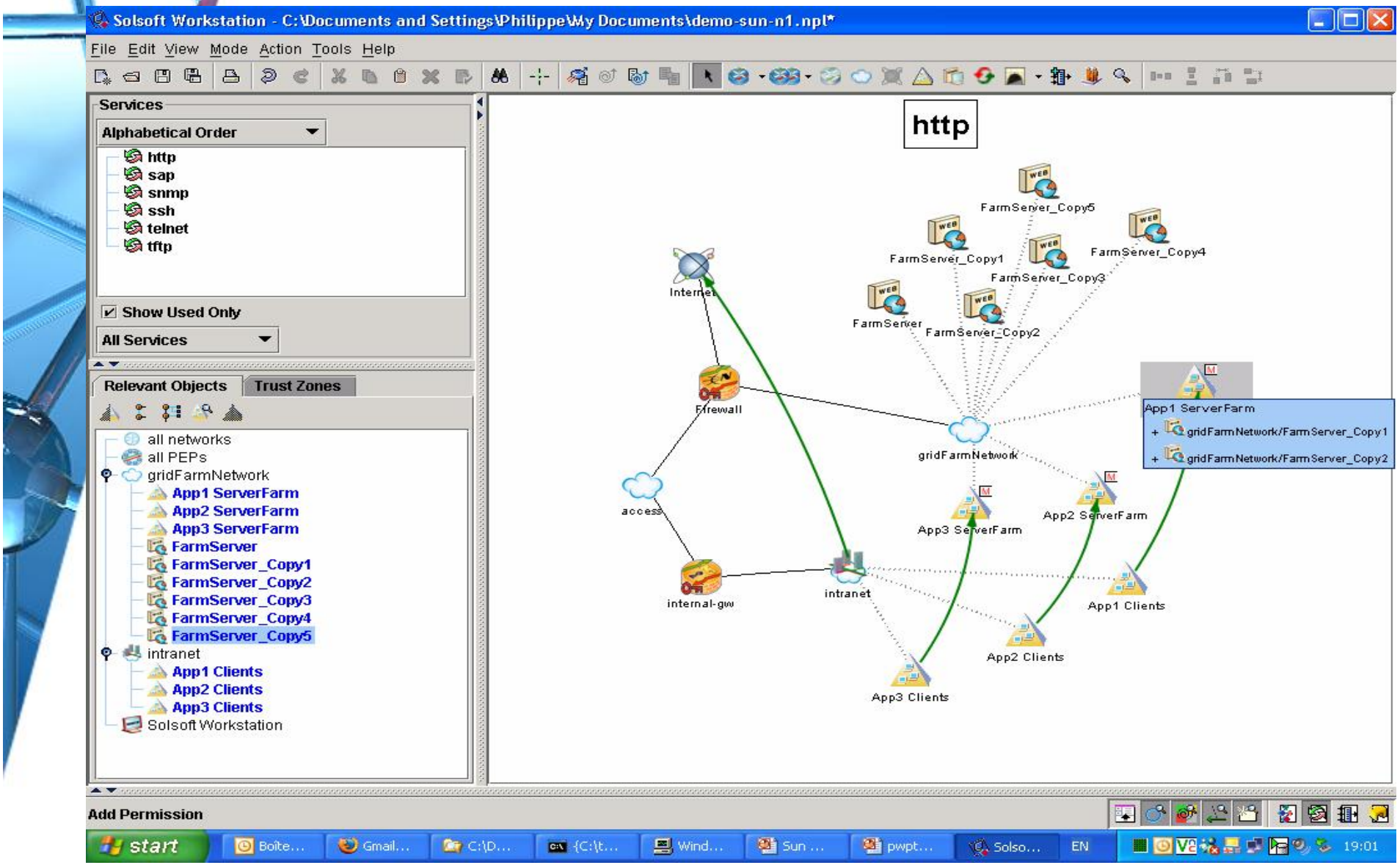
HOW SECURE NETWORKS ARE MANAGED

- **Let's demonstrate a simple example with a farm / grid application**
- **We have 3 applications:**
  - App1
  - App2
  - App3
- **We have a server farm**
  - constituted of a lot of machines with same configuration
- **We have a very diverse set of clients for each application**
  - these stay quite stable
  - Modifications to the client list is done by human action
- **Applications are deployed dynamically by GRID products on different servers of the server farm**
  - Based on request, schedule, human requests

GRID Network example

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

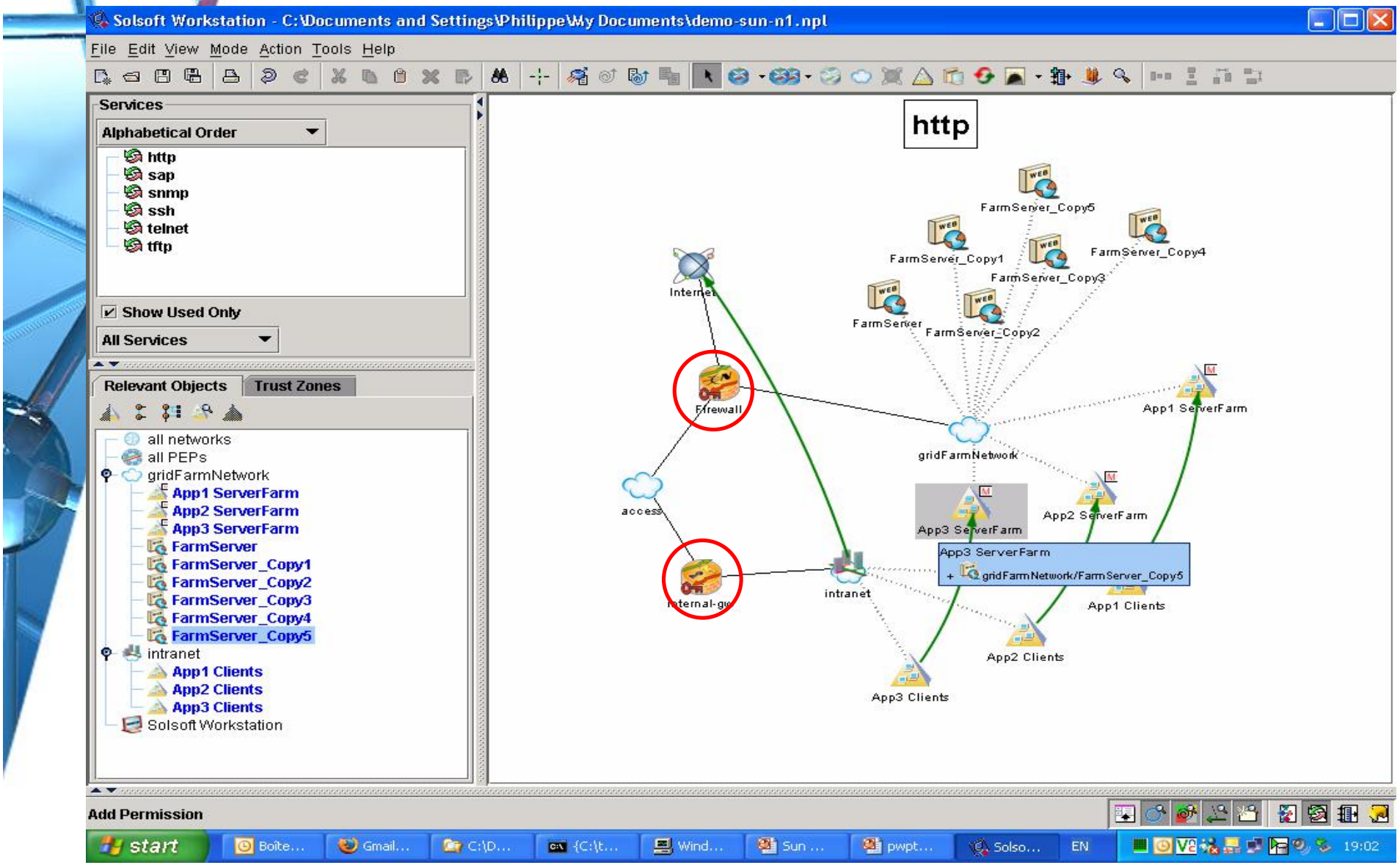
HOW SECURE NETWORKS ARE MANAGED

- **We create a template of a Grid oriented network architecture**
- **We have a server farm with several available servers**
  - FarmServer_copyX
- **3 Classes represent applications**
  - AppY ServerFarm
  - Contains one or more servers
- **3 Classes represent user groups**
  - AppY Clients
- **Users cross 2 PEPs to access applications residing on servers**
- **The goal is to have a shell script, called by GRID products which will reconfigure the two PEPs based on new application distribution on servers**

GRID Network example

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

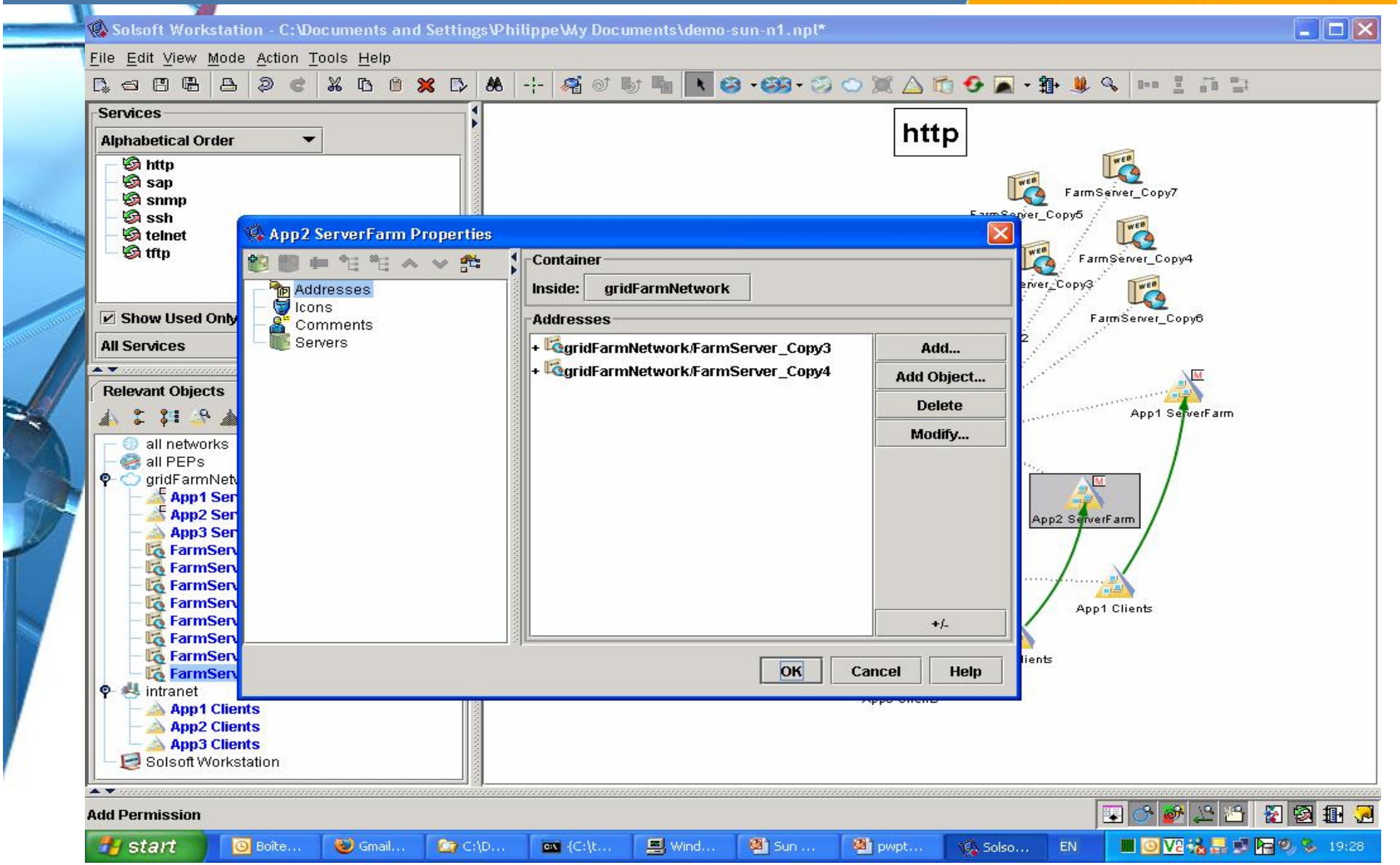
HOW SECURE NETWORKS ARE MANAGED

- **By calling our SPS Web Service API (through SOAP)**
  - You add or remove servers from application classes
  - You order re-upload of the new security policy
- **Therefore, when an application is deployed on a server**
  - Just include this server in the relevant Application Class
  - This can be done by calling a script which does all the Web Service API calls
- **Shell Example:**
  - /opt/SolsoftWSclient/addToClass -class “App2 ServerFarm” -server FarmServer_copy6 -server FarmServer_copy7

GRID Network example

SOLSOFT

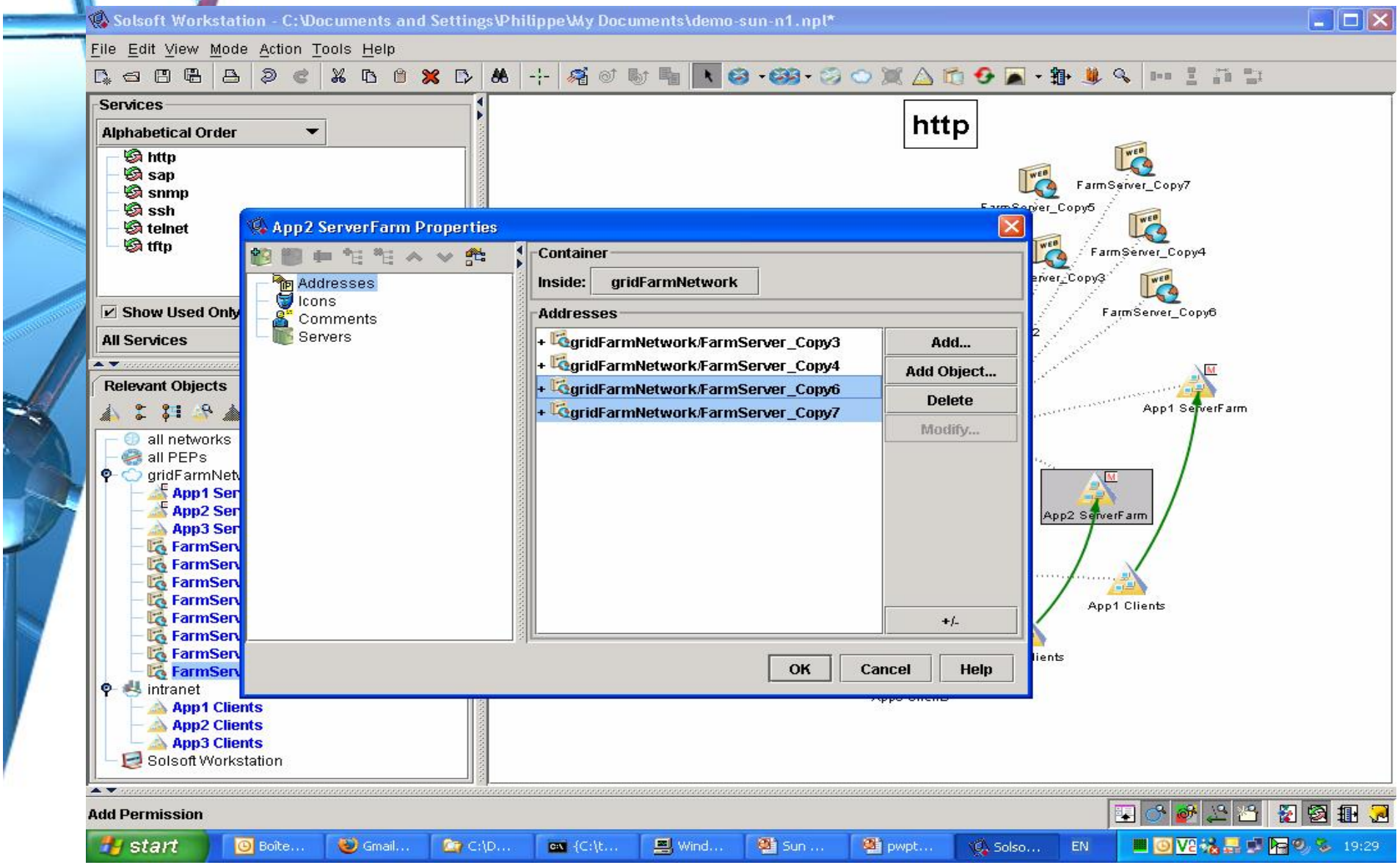
HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

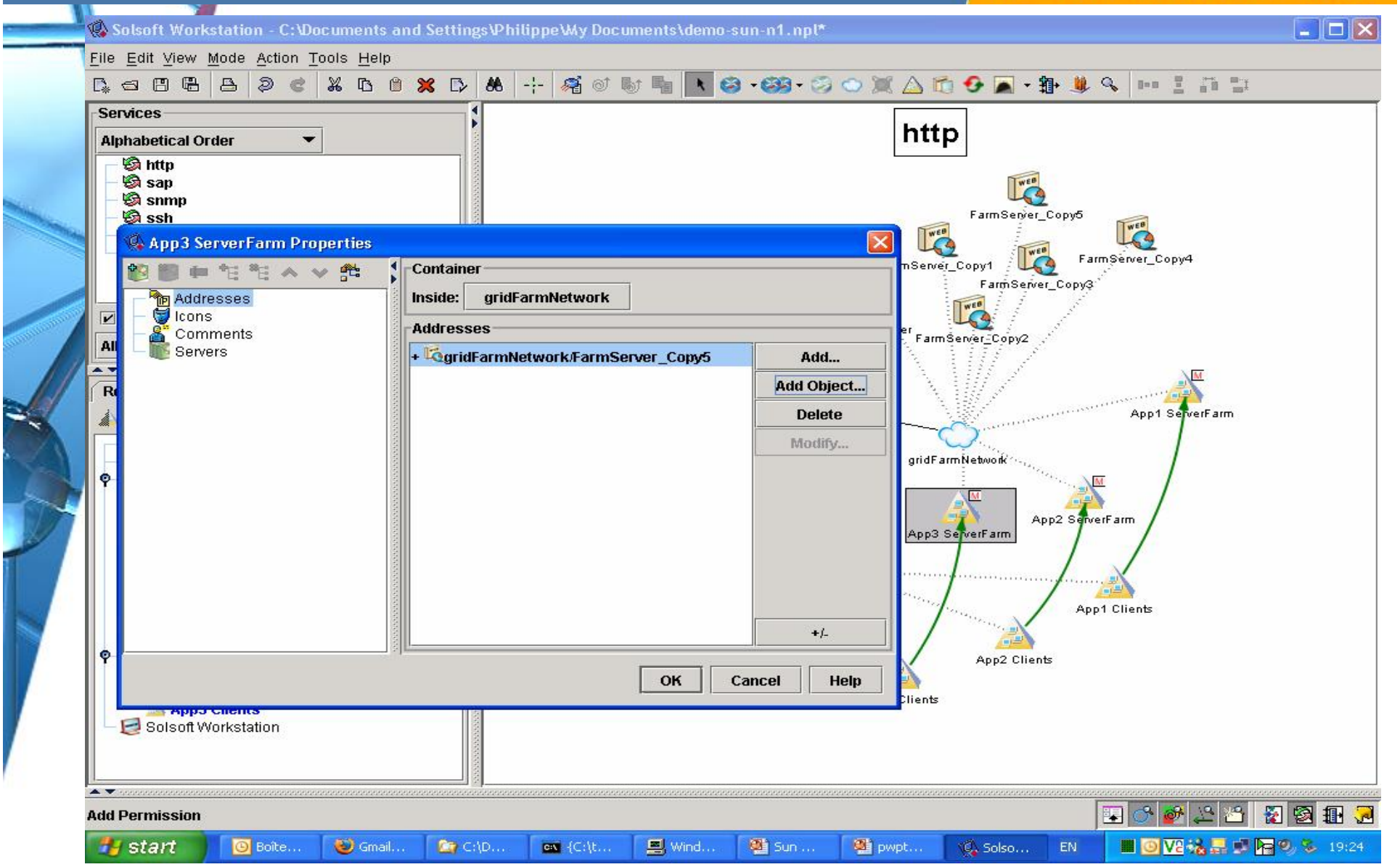
- **Same principle to remove a server from the list of server available for a specific application when an application requires less servers**

- **Shell Example:**
  - /opt/SolsoftWSclient/removeFromClass -class “App3 ServerFarm” -server FarmServer_copy5

GRID Network example

SOLSOFT

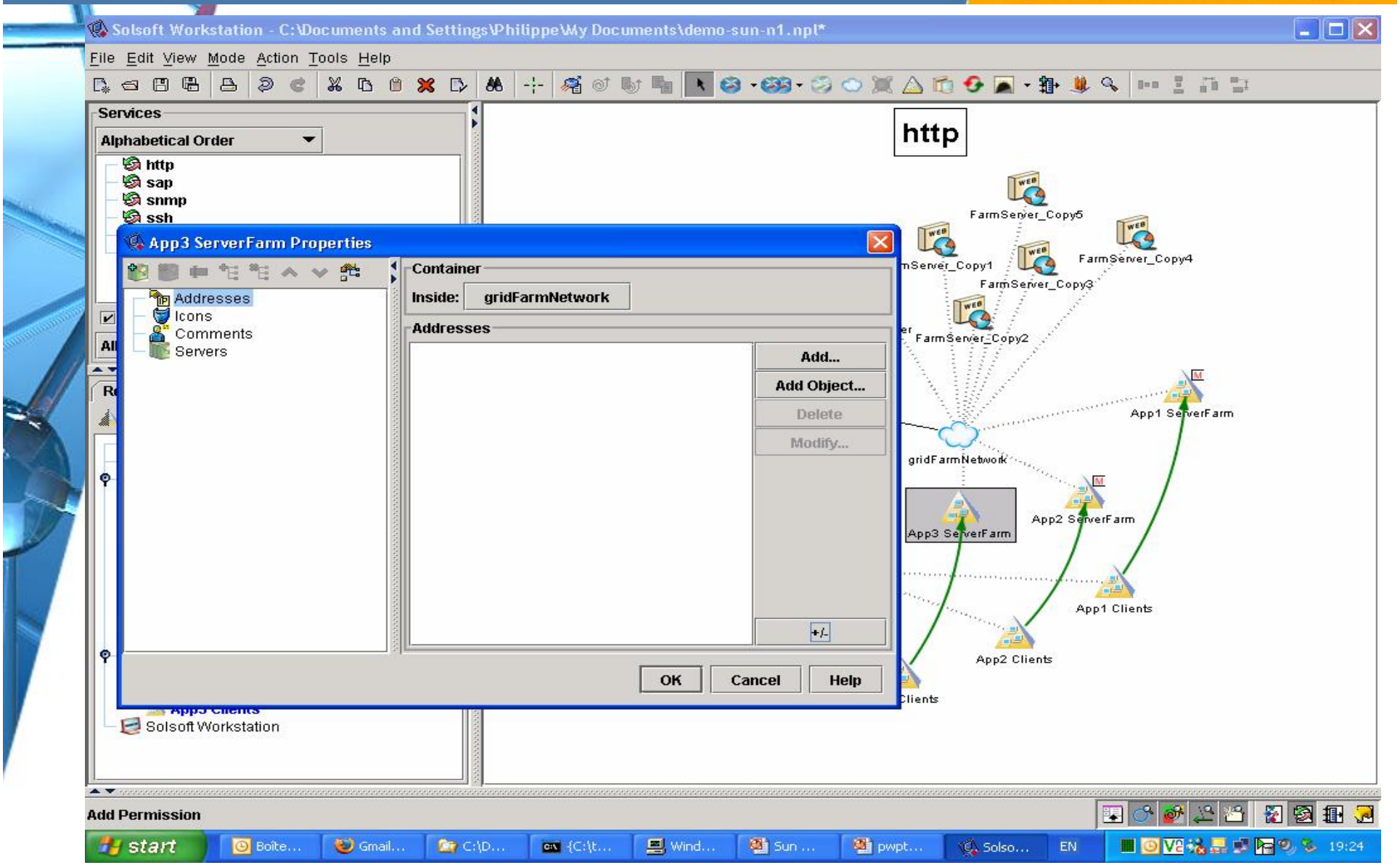
HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

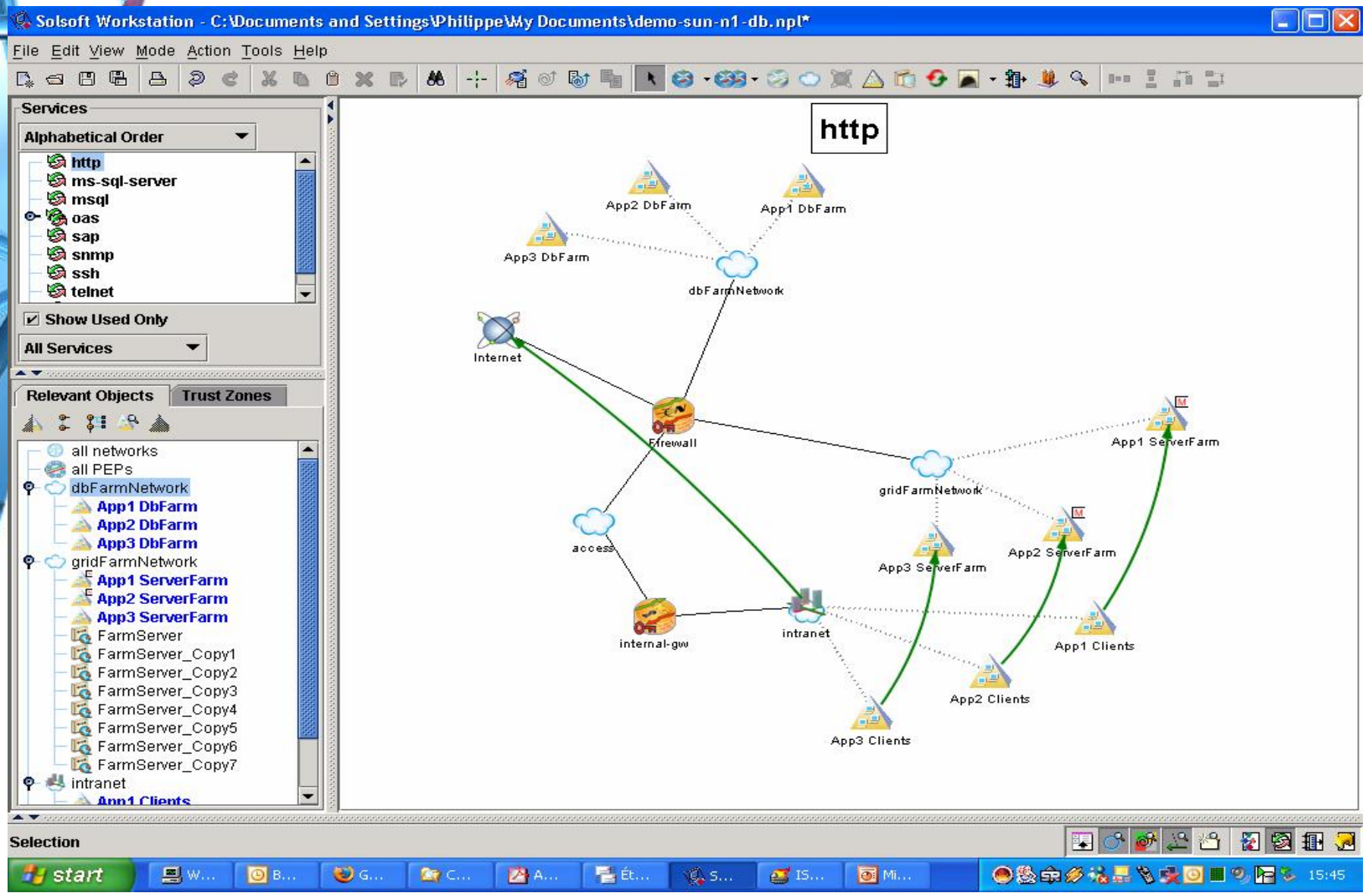
HOW SECURE NETWORKS ARE MANAGED

- **In this more advanced evolution, we want to tighten security of our whole application farm infrastructure.**
- **We thus segment Databases from Application Server, and locate them on a different part of the network.**
- **Since we reference only classes in our code**
  - We don’t need to modify our code at all to support this new infrastructure.
- **Evolutions on network topology are therefore very easy to integrate with business continuity.**

GRID Network example

SOLSOFT

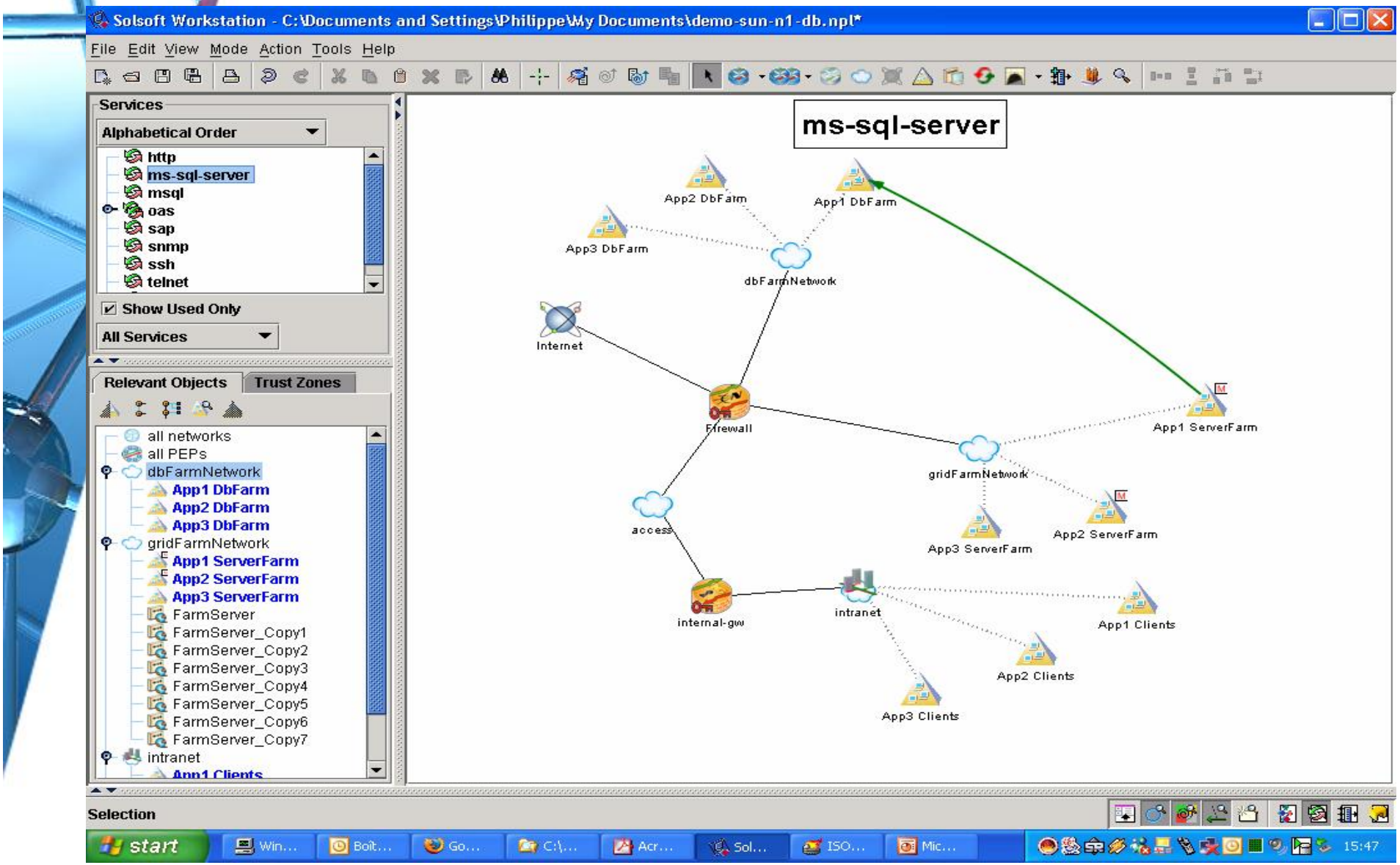
HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

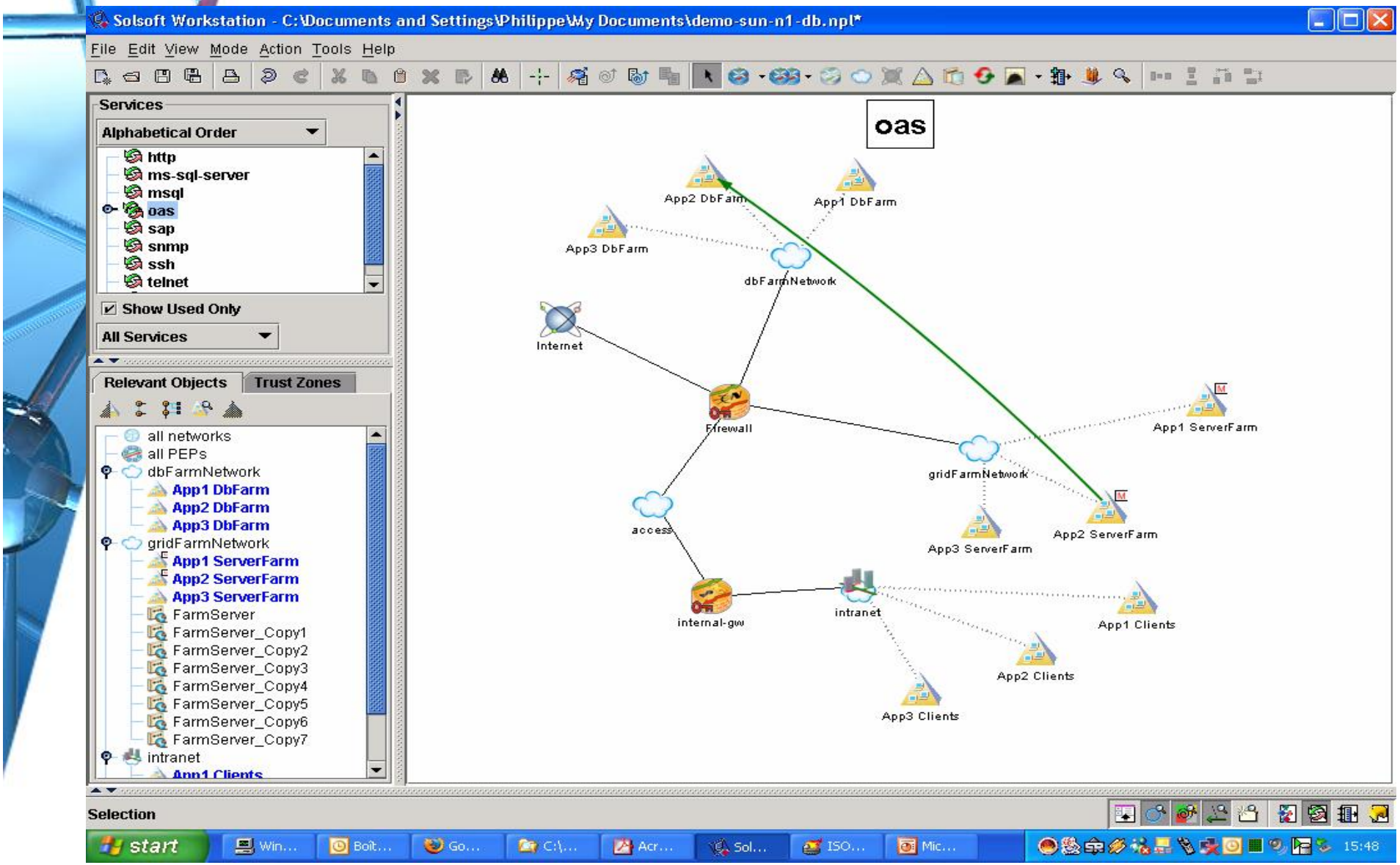
HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

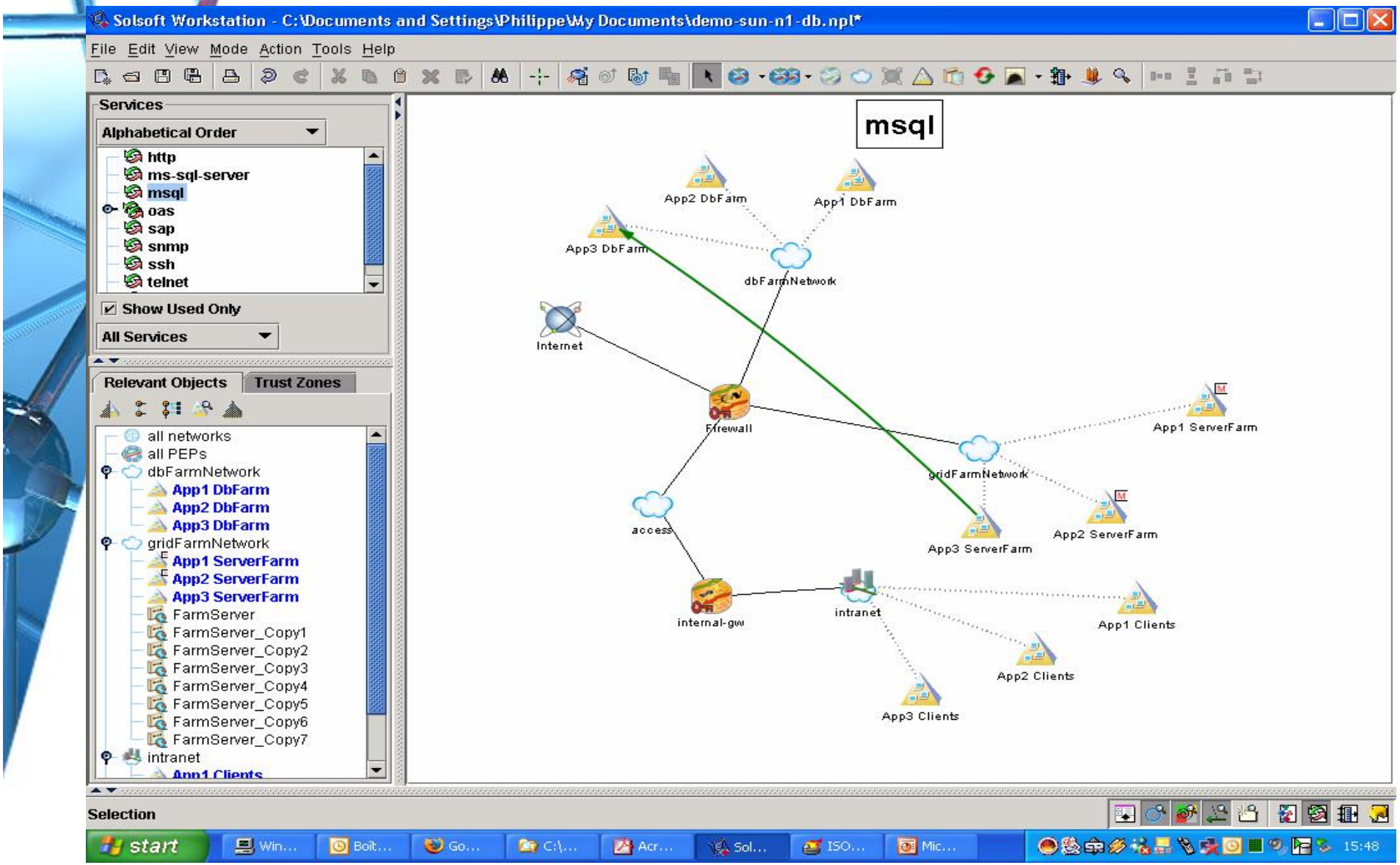
HOW SECURE NETWORKS ARE MANAGED



GRID Network example

SOLSOFT

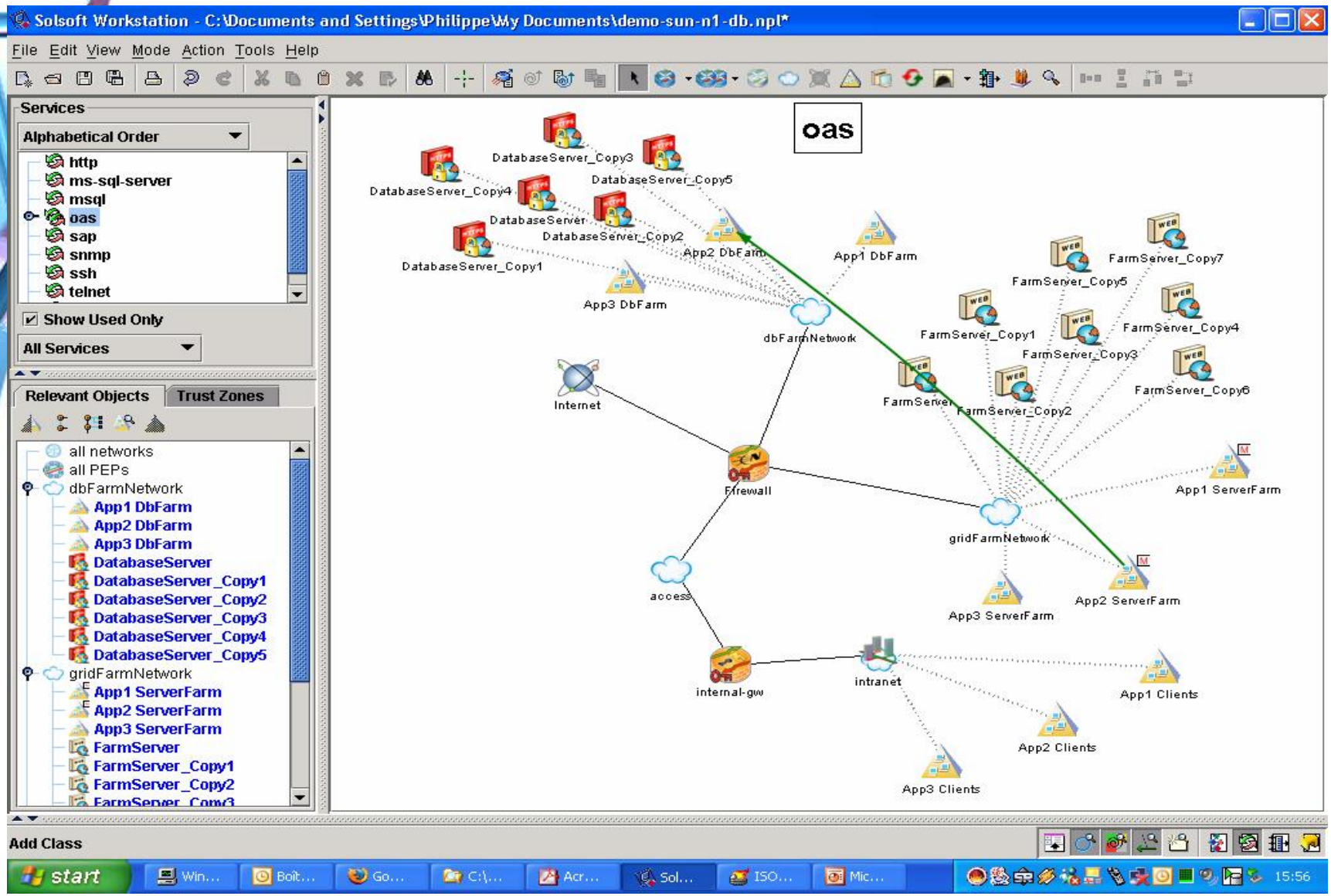
HOW SECURE NETWORKS ARE MANAGED



GRID Network example : whole picture

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



For More Information

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

www.solsoft.com

- Online demos
- White papers, brochure
- Request for evaluation

info@solsoft.com

Philippe.Langlois@solsoft.com

HOW SECURE NETWORKS ARE MANAGED

THANK YOU !

SOLSOFT

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Backup Slides

Customers Worldwide

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Financial Institutions

DOWJONES

HSBC

SELF trade
a member of DAB bank

Lombard Odier

DEXIA

VISA

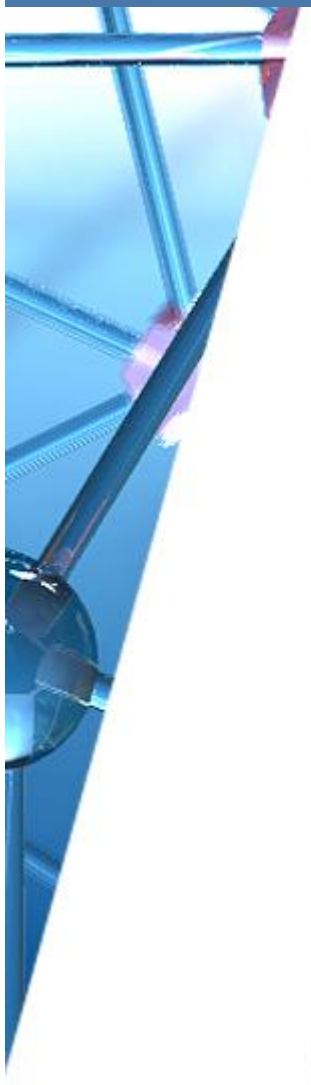
Crédit Mutuel

Firsthand

Customers Worldwide

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Telecommunications & Service Providers

Telepac
O outro nome da Internet

UMC

TELE KOM AUS TRIA

TELECOM ITALIA

INMARSAT

U.S. Cellular

BT

Deutsche Telekom

UNISYS

IBM Global Services **Consulting**

Hutchison 3G

Customers Worldwide

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Government & Education

urssaf.fr

DGA

CALTECH

UNITED STATES POSTAL SERVICE

U.S.ARMY

ina institut national de l'audiovisuel

OECD

Universiteit Leiden

HARVARD MEDICAL SCHOOL

METEO FRANCE

Customers Worldwide

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

Other Industries

VERITAS

Turbomeca
groupe snecma

DASSAULT AVIATION

Johnson&Johnson

COFIROUTE

ARIBA

ASTRA

SERVIER

LIDL

RENAULT

TOTAL

ALCATEL

NISSAN

JOHNSON CONTROLS

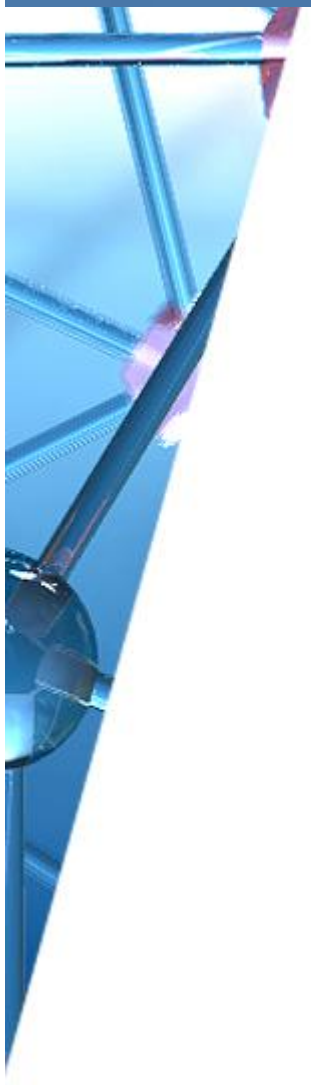
NMPP PRESSE SERVICES

ATR

Systems Integration Partners

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED



Integrators and Solution Partners

COMNET

DATACRAFT

ARCHE

Canon

DAMOVO

hp invent

IBM Global Services **Consulting**

UNISYS

ERICSSON

Netlink

steria

AXIANS

CSC

TOSHIBA

US Federal Reserve

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

The Federal Reserve Board

Challenge

- Needed a cost-effective way to expand the use of router ACLs in their network and provide a means for the Security Group to configure IP security policy in the network.

Selection Criteria

- Preferred easy-to-use, centralized policy-based solution over traditional device-based management tools.
- Solsoft enforces policy compliance and sound security practices.

Solsoft Solution

- Federal Reserve chose Solsoft to simplify the management and configuration of router ACLs and IP filtering rules on PIX and Check Point firewall devices.

UNISYS (Transportation Security Agency - TSA)

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

UNISYS

Challenge

- Find a scalable, simple, cost-effective way to manage a mixed Cisco security environment from a single user interface.

Selection Criteria

- Required the ability to manage PIX, 2600 Routers running FW/ACL and VPN.
- Wanted the flexibility to expand use of management to other vendor products without re-training operators.

Solsoft Solution

- Solsoft provided the Visual Single Management Interface across Cisco IOS routers (FW and VPN), PIX FW, VPN 3000, and Catalyst switches.
- Solsoft's vendor-neutral device support (including Check Point, NetScreen, and Nortel) gave Unisys the flexibility it needed to provide Defense in Depth designs in outer years.

What People Are Saying

SOLSOFT

HOW SECURE NETWORKS ARE MANAGED

"The Solsoft Policy Server API provides the opportunity to expand the interaction between our respective product lines. By working together, the ArcSight industry leading TruThreat™ Real Time Correlation and Solsoft Policy Server can close the gap between problem discovery and response, an area of great interest to our customers."

- Hugh Njemanze, CTO and Senior Vice President of Research and Development, ArcSight

ArcSight ESA Enterprise Security Alliance™

"Network Intelligence leads the market in appliance-based Security Event Management (SEM) and we can capture, analyze and manage logs produced by the entire Solsoft product line. Using multi-variable analysis, the enVision™ real-time correlation engine can intelligently detect actual security or network hazards and then automatically send specific tasks to Solsoft Policy Server through its new API for immediate action."

- Mr. Lynn Mormann, CEO, Network Intelligence

Network Intelligence CORPORATION