]HackingTeam[	Electrolux

Electrolux Bluecoat Director

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

DOCUMENT HISTORY		
Version	Date Issued	Action
1.0	21/12/2006	First draft

DOCUMENT DETAILS	
Date Issued	21/12/2006
Version	1.0
Document type	Technical document
Pages	22
Attachments	0
Written	Andrea Cariola
Approved	Gianluca Vadruccio

TABLE OF CONTENTS

1 Objective

The aim of this document is to describe the solution based on *"Bluecoat Director"* appliance to control and centralize all maintenance operation of all Bluecoat appliances distributed over the Electrolux network infrastructure.

This implementation will give the customer the ability to centrally manages and monitors all aspects of a network where Blue Coat Proxy*SG* Appliances are used. Administrators can use Director to set user and content policy, manage ProxySG Appliance configurations, distribute and control all types of Web content, and back up Proxy*SG* Appliances.

2 Target environment

The environment mainly involved in this phase is composed by three hub customer sites: *Pordenone, Stockholm and Nurnberg*.

Each of these hub sites has its own Internet link and each site communicate with others through the provided carrier VPN.

The scalability of the solution will eventually permit to expand and include other customer sites where necessary using the same methodology.

The Bluecoat appliances the customer will include under the control of *Bluecoat Director* are forward proxy as well as reverse proxy.

Target environment is outlined below (Fig. 1**)**. Please note that this schema doesn't pretend to be exaustive, but has the only aim to formalize technological context in witch the offer will be valid

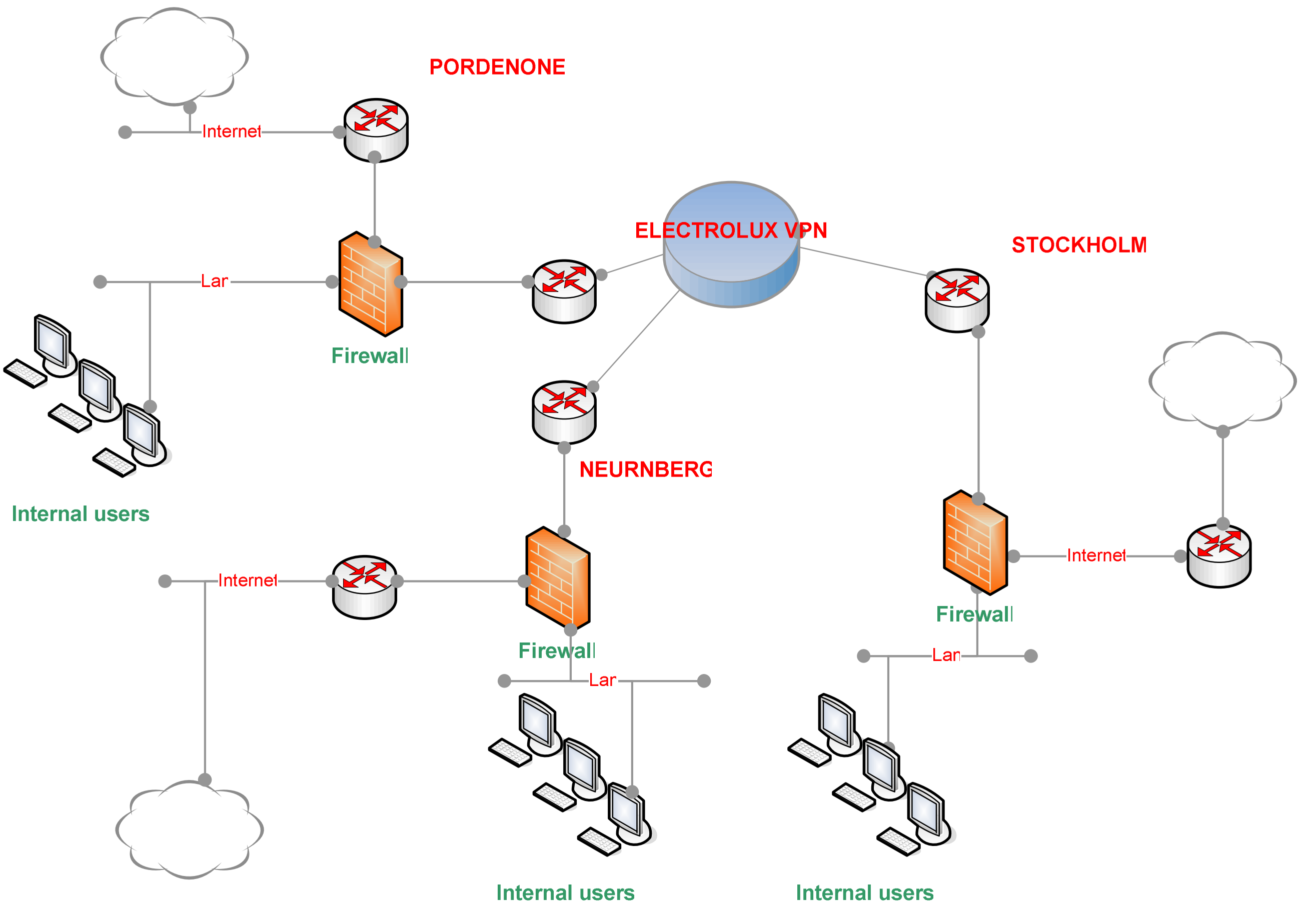


Fig. 1

3 Solution description

This paragraph describes, from a technical point of view, the architecture and characteristics of the Bluecoat Director solution that will be installed in the customer's infrastructure located in Pordenone and that will serve the whole emea Bluecoat proxy infrastructure.

3.1 Implemented hardware and functionalities

The proposed solution is based on the Bluecoat Director appliance model 510 that enables the customer to have a solution valid for the actual supposed ProxySG Emea architecture (forward and reverse proxies).

3.1.1 Bluecoat Director Overview

Blue Coat Director delivers scalable configuration, and policy management for Blue Coat proxy appliances.

Director reduces administration complexity by providing a platform for centralized management of Proxy*SG* appliances. Configuration information and security policies are created and managed from a single interface available from any workstation with a Web browser and Director Management console software installed.

In particular, the main peculiarities of Bluecoat Director are dealing with centralized, network-wide policy-based management that lets do:

- Automated software upgrades
- Configuration backups and disaster recovery
- Powerful job scheduling automation
- Management appliance for simple install and ongoing maintenance
- Manage remotely via secure GUI or CLI
- Develop and manage policy centrally, distribute globally
- Launch and use from any workstation with a Web browser
- Reports give visibility into job status and outcomes
- Pre-position content as needed using scheduled or immediate actions

Centralized Policy Management

Blue Coat Director automates change, policy and configuration management. It enables enterprises to easily standardize the configuration of Blue Coat proxy appliances, creating policies that can be globally applied or customized by region or to a logical group of appliances. By leveraging a single point of administration, IT staff no longer need to “touch” every device, allowing to effectively manage new threats in a timely manner.

Key management features include:

- Rapidly configure and deploy new devices
- Easily upgrade installed systems
- Centrally manage new policies and configurations by device, group of devices, or region
- Proactively manage the network to prevent problems
- Conserve valuable network resources with bandwidth policies and content pre-positioning

Configuration Management

IT staff can deploy and configure new devices with Blue Coat Director. Using templates, administrators can standardize device configurations easily–and still customize them based on region or device-specific settings.

Blue Coat Director also automates software and license upgrades, ensuring version consistency and schedule updates during off-peak hours. Distribution sources can be located anywhere on the Internet or within an organizations intranet. With the combination of templates and overlays, organizations can ensure network consistency, as well as customize appliances by region or application. Director can centrally store configurations and coordinate their downloads from regionalized sources. For powerful automation, configurations can also be distributed and scheduled as CLI, scripted commands.

Blue Coat Director also keeps backups of all appliance configurations and policy settings, making it simple to rollback to known good configurations if a system problem does occur. Configuration snapshots can be scheduled, created before changes are applied, or based on standardized templates.

Policy Management

With Blue Coat Director, administrators can centrally create and manage security and user access policies. The need to respond to new threats or make a policy change can occur at any time. When this occurs, updating all the security policies immediately is critical. Administrators can use the Visual Policy Manager to create policy on the Director and distribute the change when it’s needed, rapidly and effectively. Multiple policy templates can be stored and managed on the Blue Coat Director, making it easy to customize policies based on region, workgroup, or other characteristics. For more advanced users, policies can also be automated and distributed based on the Content Policy Language (CPL).

Resource Management

To conserve valuable network resources, Director allows creation of bandwidth policies and pre-position content on Proxy*SG* Series appliances. As part of a comprehensive bandwidth management strategy, proactively positioning high-bandwidth content such as streaming media or large static files allows enterprises to control the impact of those files on the network. Content can be distributed, prioritized and scheduled based on the complete range of policies supported by Director.

Proactively Monitor and Plan

Director also allows administrators to monitor device status and statistics from a centralized Web-enabled GUI. Blue Coat Reporter, enables running of reports on security problems, usage patterns, and network traffic flows, allowing proactive evaluation and updating of security policies.

Easy to Deploy and Maintain

Optimized as a management appliance, Blue Coat Director can be remotely managed via both a graphical user interface (GUI) or command line interface (CLI). The GUI console allows easy management and fast deployment. The CLI–which can be accessed via serial console, Telnet, or SSH–allows easily programmable automation, quick troubleshooting, and fast remote access, via secure network protocols.

3.1.1.1 Director's solution components

The Fig. 2 below shows the elements composing the typical Director architecture.

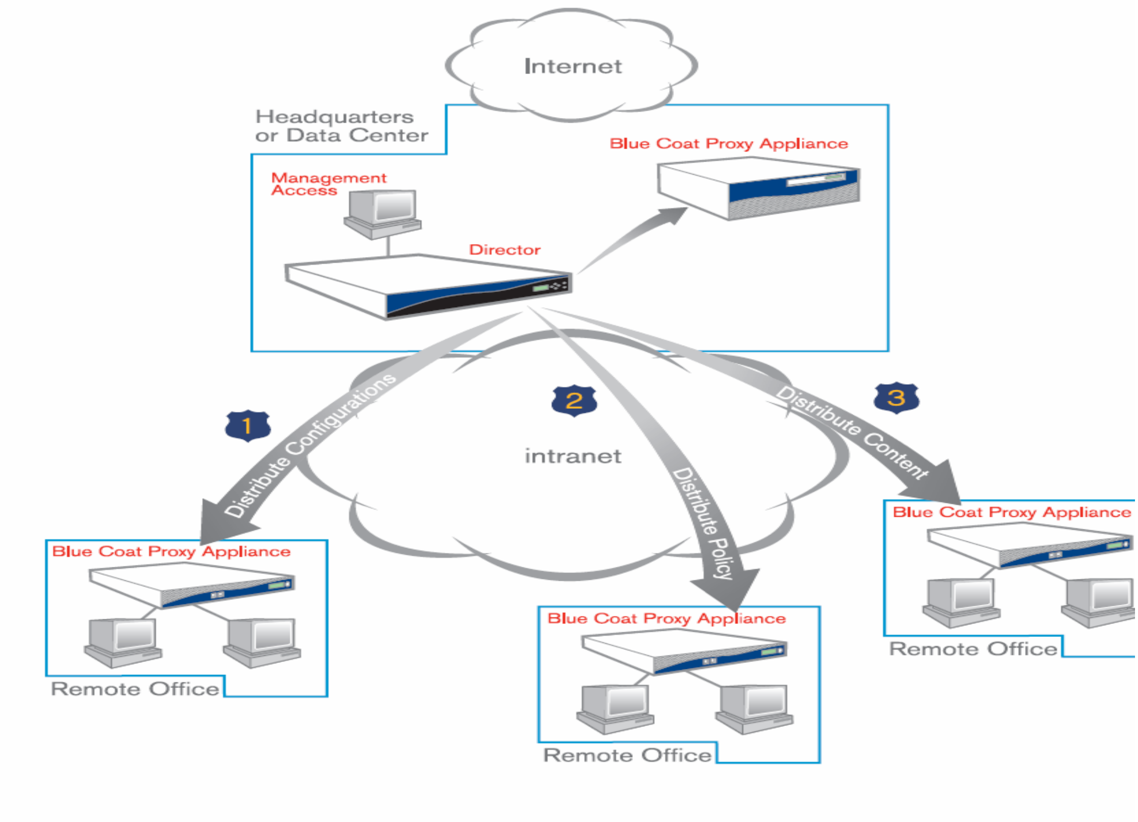

Internet
Headquarters or Data Center
Management Access
Director
Blue Coat Proxy Appliance
1
Distribute Configurations
2
intranet
Distribute Policy
3
Distribute Content
Blue Coat Proxy Appliance
Remote Office
Blue Coat Proxy Appliance
Remote Office
Blue Coat Proxy Appliance
Remote Office

Fig. 2

The main elements are:

- *Bluecoat Proxy SG appliances*

  These are all Bluecoat ProxySG appliances across the network; can be forward proxies as well as reverse proxies
- *Bluecoat Director appliance*

  This is the appliance for configuration and policy management of Blue Coat Proxy*SG* appliances
- *Bluecoat Director Management console*

  This is a software component that is needed to manage multiple management nodes and the Blue Coat SG appliances added to them.

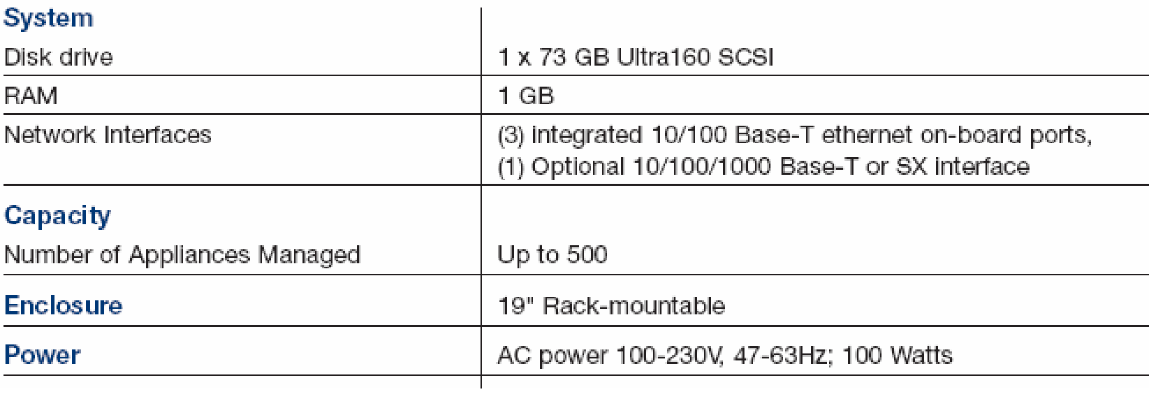
  It have to be installed on the PC designated to interact with Director appliances

These components can be distributed across the enterprise, communicating across company intranet or other links.

3.1.2 Bluecoat Director infrastructure sizing and requirements

The sizing of the Director architecture refers to appliance hardware and management console software requirements.

Director appliance configuration and specification chart



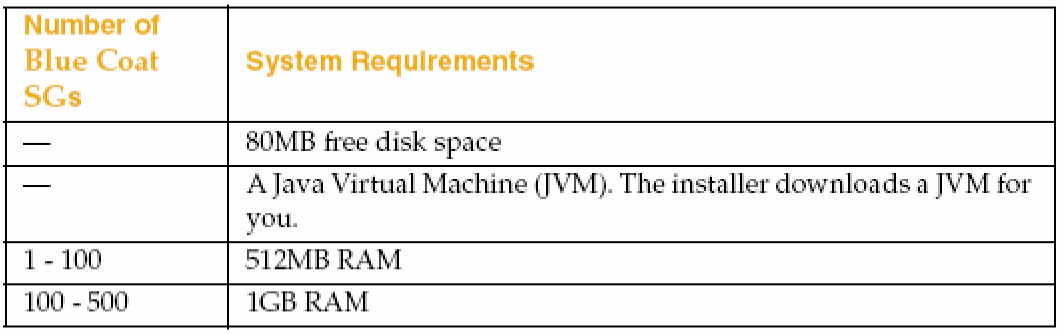
System	
Disk drive	1 x 73 GB Ultra160 SCSI
RAM	1 GB
Network Interfaces	(3) integrated 10/100 Base-T ethernet on-board ports, (1) Optional 10/100/1000 Base-T or SX interface
Capacity	
Number of Appliances Managed	Up to 500
Enclosure	19" Rack-mountable
Power	AC power 100-230V, 47-63Hz; 100 Watts

Director Management Console System Requirements

The Director Management Console uses the following software/O.S. :

- Microsoft 2000 Pro (SP2 or later), XP (SP1a or later)
- Internet Explorer 6.0 (SP1 or later), Firefox 1.0, Netscape 7.2
- JRE 1.5.0_06 is the supported Java Runtime Environment for Director and is downloaded with Director on an upgrade.

The client PC running the Director Management Console has different requirements depending on how many Blue Coat SG appliances are controlled; see the Fig. 3 System Requirements for Director Management Node below for further details:



Number of Blue Coat SGs	System Requirements
—	80MB free disk space
—	A Java Virtual Machine (JVM). The installer downloads a JVM for you.
1 - 100	512MB RAM
100 - 500	1GB RAM

Fig. 3 System Requirements for Director Management Node

3.1.3 Management Architecture of Director

This chapter illustrates the main components of the managing architecture of Bluecoat Director solution and how they can do various tasks needed by administrators.

3.1.3.1 Configuration Management

Director automates configuration and policy management to one or more Proxy*SG* Appliances from a single point of administration. It manages everything from Proxy*SG* Appliance configuration to policy and license distribution.

Key configuration management features include:

- Configure groups of Proxy*SG* Appliances based on locations, applications, or more.
- Rapidly deploy standardized configurations using profiles.
- Manage the scheduling of policy and configuration changes.
- Easily schedule incremental changes to one or more Proxy*SG* Appliances
- Create and distribute policy across a system of Proxy*SG* Appliances.
- Automatically back up configuration snapshots.
- Back up Proxy*SG* Appliance backup files.
- Compare backup files from different Proxy*SG* Appliances and restore configuration backups to multiple Proxy*SG* Appliances.
- Quickly monitor Proxy*SG* Appliance status, statistics, and configurations.
- Upgrade all Proxy*SG* Appliances at once.

3.1.3.2 In-Progress Querying

Director provides querying and reporting of Director commands while they are in progress. You can query each pending command for summary and detailed status on a Proxy*SG* Appliance/group basis, a URL/regex basis, or a command ID basis.

3.1.3.3 Job Scheduling Functions

This feature permits to create job scheduling and Proxy*SG* configuration functions on a per Proxy*SG* Appliance or group on a recurring or one-time basis. One-time or recurring jobs can be scheduled for a specific time and date.
All these actions can be done from Director Management Console or Director CLI. Within each of the above-listed activities (distribute, delete, revalidate, and set priority) it is also possible to do the following:

- Set up jobs for repeating actions ("Scheduled Content Jobs", discussed below).
- Execute jobs one-time only ("Immediate Content Jobs", discussed below).

Scheduled Content Jobs
Scheduled Content Jobs let the administrator do content management actions that need to be done repeatedly, such as deleting old content from specific Proxy*SG* Appliances or groups on a daily basis. To achieve this, it is only needed to create the actions required once and then put them into an automated schedule to be done on days and times that you specify. It is also allowed to create a job that is only scheduled to run once.

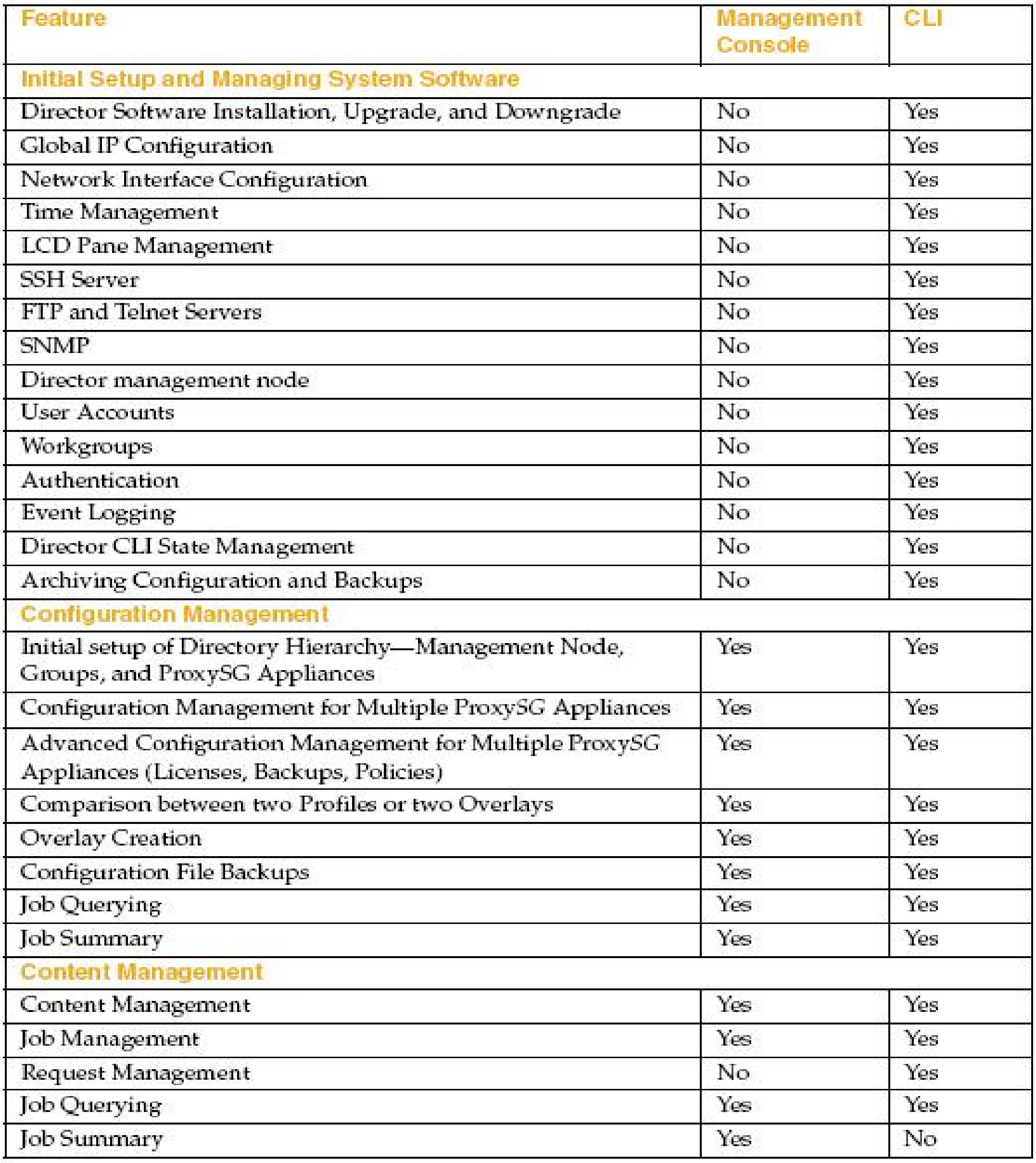
Immediate Content Jobs
Immediate Jobs let the administrator do one-time content management actions, such as deleting old content. Immediate Job actions are not put into a schedule, but can be done on an as-needed basis. Immediate Job requests are remembered by Director only for the length of the session. Once the Director Management Console is closed and relaunched, the job request is not remembered and must be re-created if it have to be used again.

3.1.3.4 Director Management Console and CLI

Director allows to use either the Director Management Console or the CLI to manage Proxy*SG* Appliances. The Director Management Console provides a graphical view to complete configuration tasks quickly.

The Director CLI is used primarily for initial setup of the Director management node and Proxy*SG* Appliances. Once Director is set up, is possible to rely primarily on the Director Management Console.

Table 1 below lists the actions that can be done in each interface.



Feature	Management Console	CLI
Initial Setup and Managing System Software		
Director Software Installation, Upgrade, and Downgrade	No	Yes
Global IP Configuration	No	Yes
Network Interface Configuration	No	Yes
Time Management	No	Yes
LCD Pane Management	No	Yes
SSH Server	No	Yes
FTP and Telnet Servers	No	Yes
SNMP	No	Yes
Director management node	No	Yes
User Accounts	No	Yes
Workgroups	No	Yes
Authentication	No	Yes
Event Logging	No	Yes
Director CLI State Management	No	Yes
Archiving Configuration and Backups	No	Yes
Configuration Management		
Initial setup of Directory Hierarchy—Management Node, Groups, and ProxySG Appliances	Yes	Yes
Configuration Management for Multiple ProxySG Appliances	Yes	Yes
Advanced Configuration Management for Multiple ProxySG Appliances (Licenses, Backups, Policies)	Yes	Yes
Comparison between two Profiles or two Overlays	Yes	Yes
Overlay Creation	Yes	Yes
Configuration File Backups	Yes	Yes
Job Querying	Yes	Yes
Job Summary	Yes	Yes
Content Management		
Content Management	Yes	Yes
Job Management	Yes	Yes
Request Management	No	Yes
Job Querying	Yes	Yes
Job Summary	Yes	No

Table 1

The graphical user interface is Director's Management Console, running on Microsoft Windows. The Management Console administers multiple Director domains as well as the Proxy*SG* Appliances associated with the domains.

In order to communicate with the Proxy*SG* Appliances and the Director management node(s), the Director Management Console must know the hostname or IP address of the management node. (it is possible to have more than one management node on the Management Console.) The Director Management Console communicates with the management node via an SSHv2 (by default) or Telnet protocol.

The Management Console contains several windows to manage Proxy*SG* Appliances for one or more Director management nodes:

- *Main window*

  Within this component it is possible to set up the Director domain (management node): adding Director management nodes, adding Proxy*SG* Appliances and Proxy*SG* Appliance groups, and modifying the properties of management domains and Proxy*SG* Appliances (hostname, type of authentication used).

- *Quick View/Edit window*

  The Quick View/Edit window offers a quick and convenient way to modify an individual Proxy*SG* Appliance. It allows you to change configuration settings and view statistics on a single Proxy*SG* Appliance.

- *Configuration Management window*

  The Configuration Management window allows you to centrally manage configuration for a Proxy*SG* Appliance or group of Proxy*SG* Appliances on a specific Director management node, and duplicate those updates on other Proxy*SG* Appliances simultaneously. It is also possible to:

  - Create backups of Proxy*SG* Appliance configurations, and save the backups, optionally allowing them to be rotated out after a certain amount of time.
  - Back up Proxy*SG* Appliance configuration files.
  - Compare backup files and profiles from different Proxy*SG* Appliances.
  - Restore configuration backups to multiple Proxy*SG* Appliances.

  - View configuration and backup job results (content job results are viewed from the Show Query windows).
  - Schedule configuration jobs.

- Several windows to manage content
  The Content windows allows to manage content from the Management Console such as distribute and query (content to Proxy*SG* Appliances), delete, revalidate (make sure the content is still fresh) and prioritize (set the importance of the object in the Proxy*SG* Appliance in comparison to other objects in the Proxy*SG* Appliance) contents. Each of these actions can be putted into a schedule and run at any designated time. It is alto possible to do actions on the fly without putting them in a schedule.

3.2 Electrolux proposed solution details

This chapter outlines the discussed solution for customer environment; all this is based on requirement analysis and on chosen technology constraints.

Even if the Electrolux final target environment will evolve in next month, increasing the number of sites and branch offices that will use Bluecoat appliances, the proposed solution is scalable and can cover the previewed growth.

3.2.1 Component architecture

The Fig. 4 below shows the Bluecoat Director implementation based on the Electrolux *"target environment"* described in network topology of Fig. 1.

At the moment the installed Director is interacting with Electrolux Proxies in Pordenone because the absence of other ProxySG appliances.

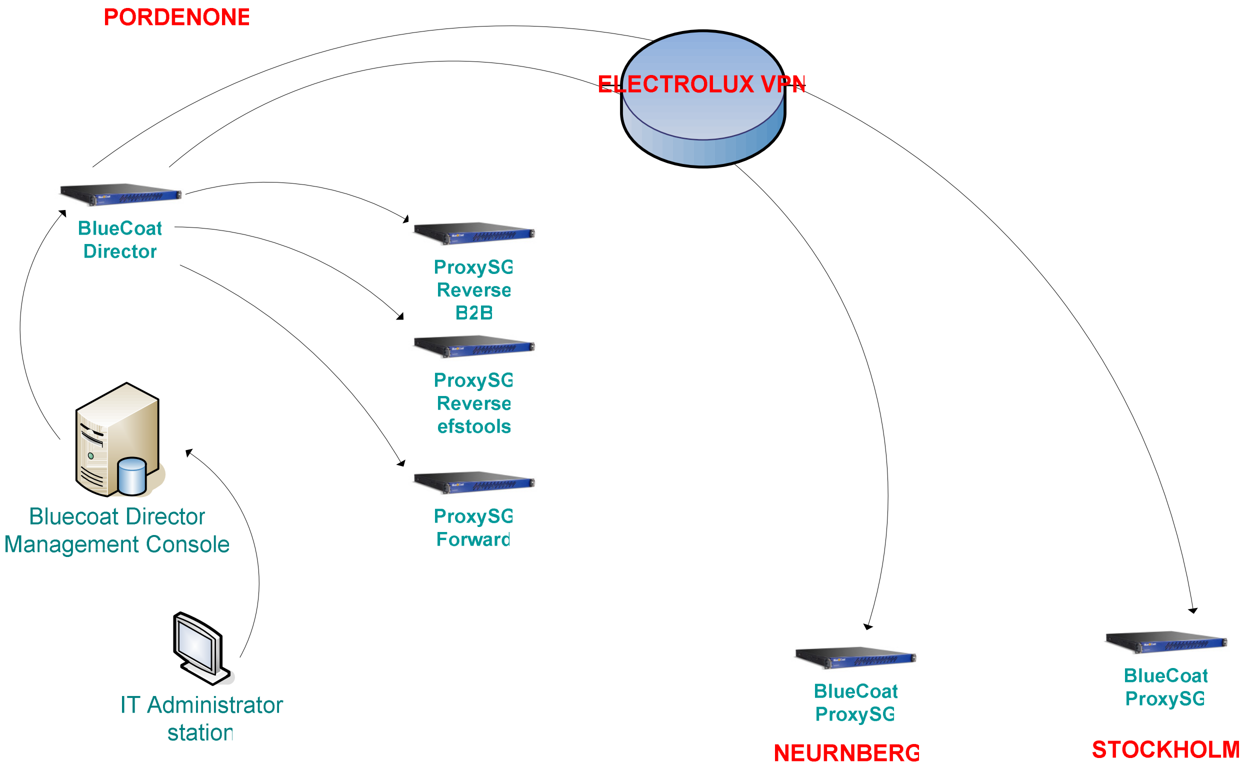


Fig. 4

3.2.2 Integration of Director with other Bluecoat components

This chapter explains the current implementation of Director for Electrolux Pordenone. The following Fig. 5 represents the configured solution:

PORDENONE

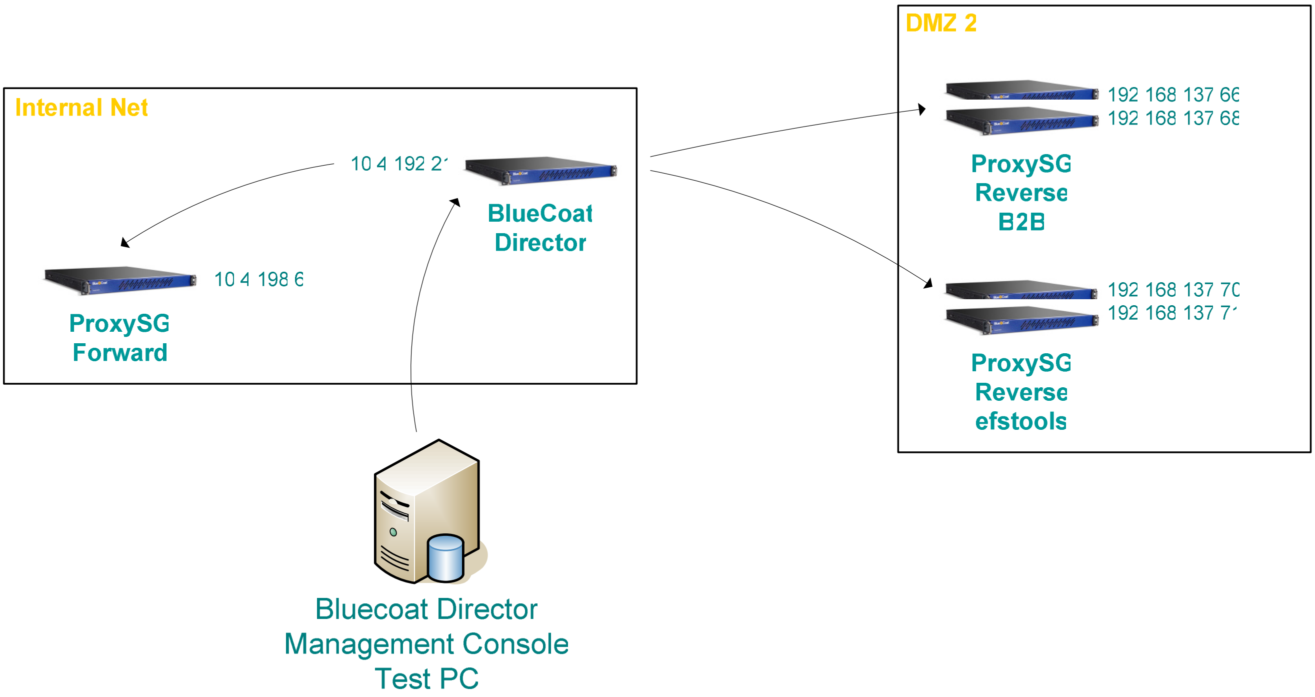


Fig. 5

3.2.2.1 *Bluecoat Director basic (CLI) configuration*

Network parameters

The appliance is placed in Electrolux Internal Network and is configured with the following network parameters:

IP ADDRESS	10.4.192.21
NETMASK	255.255.254.0
GATEWAY	10.4.193.245
DNS SERVER 1	10.4.192.49
DNS SERVER 2	10.4.192.50

Oerating system version

The O.S. was updated to *"SGME 4.2.2.1"*.

Administrative credentials

The username for accessing the unit is “admin” and the password was chosen by the customer. This credentials are valid to access the Director appliance via SSHv2 as well as via the “Management Console Software”

3.2.2.2 Director configuration archiving setup

It is possible to backup and restore Director configuration files, event logs, job reports, and Proxy*SG* Appliance backups through the archive utility. These backups can be archived to another server in the network as long as the server is network-accessible to Director.

The *“config archive”* commands (used to perform the tasks described in this paragraph) are memory and disk intensive. A temporary copy of the configuration is created before archival. Blue Coat recommends to purge unwanted backup and configuration files from the Director before creating an archive.

Please consider that the following ProxySG configurations parameters:

- ip-default-gateway
- interface (the entire submode)
- line-vty (the entire submode)

are not included in the “*archive*” and in case of proxy appliance replacement they have to be manually inputed.

Because archives are encrypted, the first step in creating an archive is to provide an encryption key that should be used whenever you archive Director files.

The *generated keypair* are the following:

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMrayHWFDnPTcx1cFdysfRPf8D
Xf3zfI9foHsWRmVlArirJHE0cp+M0rwLvPECtyYB/9fVGWcLlg1uc+9Y/Hy7d4gL
4aJP3i7Vpo/Q49PJTe14ua3aUKWpRruMc2mbDZynfxVH2y53UpeSPGm5/8ljNF31
HtCNxWUr9ulBdstk1QIDAQAB
-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
```

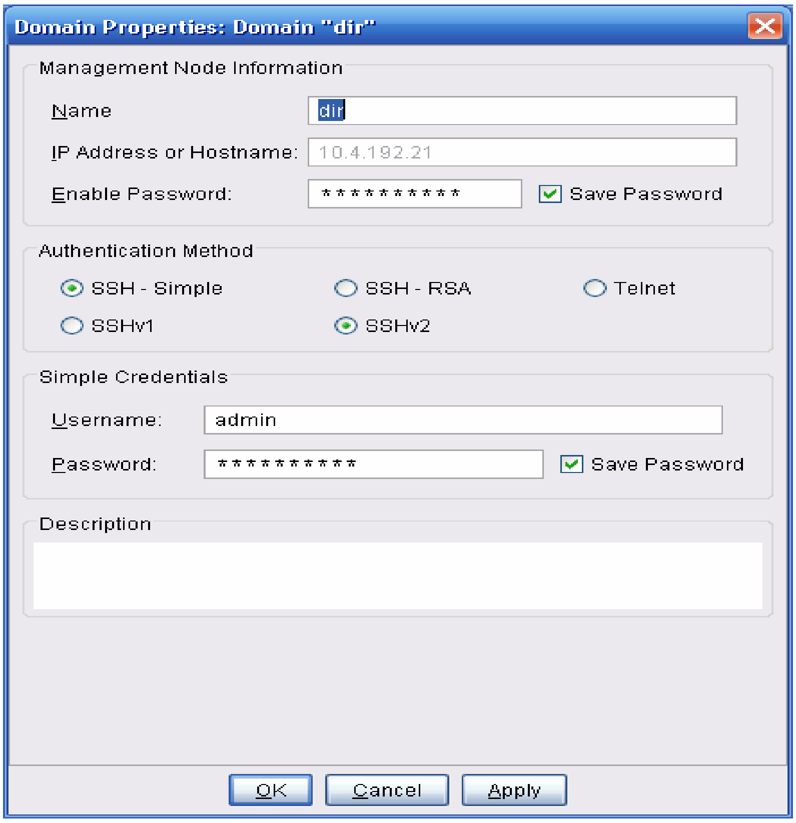
```
DEK-Info: DES-EDE3-CBC,884536293D14791A

ICL4G1ymwudyfdTBK+Gt4PQHgL+nsozQ32CuVsCwXnvwGgOgU3obqOIh6FoooEb4
iQxOpMmLvq0xZ9MZMtN+qa/FTW40UnHOcC1ol+gqJJ58DIyvQKYiZbSGV2bySale
+GcNdw7p0abeCXsthYr72siQuICLj0imM/EJ1wS5qXWfFjaTESHNGu7J4sjIO/Mr
7epwm5v3kubEP6Q0XKZOONTYqs2fjZy7+Lt6mRsEGOZxpXAB4KsgSXqKB/y+lr6r
pjh6c+kWplfd0Nnyx9YUpfdkr9gLVa2j7rmGaBTWtNoP3bpaVR9z7qVKiX450hJa
mLhUvzEYe0AxSaEMvCSQenrlJjsZSlzSvpxqzaw0gQBc2SWFjlSJj2TttjIwJKEE
5LHr9R2TteGWvPW3OtLPgAKRjdynW2ngGwaGATKI7BHXUEbC1/37v1KH0KvbPyek
ulokwmZIYu032Ln8t9Q1CMQ/CZB/pKYKzdbjZWb3UVOS4Ju1oPUS7Cp2/aFNcGVl
Ekuf9OtVZmaFNG0aVk9abA1UpwSJ8esEMNI4KemQGoq4dJGea98odqKFUqELDBgG
JO7rVwdh/3fR/AjsQ8b1yZabOakdNeTpvFINPSf2CYSLMwXw8EbcMMj53a+e2u9y
UiUbO8UAH791bf33XN4UxiNiNcow7TE3jAAVvFwylLevxhgIRcfSy+Y7ieBbUT83
JgCBEGsf3b9r4YVr1s8OgQJy1vCx+IuRgFxcd2BAC/bmHSB/zjXJc4/Qkq4PigdK
Se5dkFvgQmM7weI6GyxzuOvI0YUf65XTzLey6o1e1Rfzm5QEaomUhw==
-----END RSA PRIVATE KEY-----
```

The *passphrase* used for private key is the same as the *admin password* used before.
This informations have to be used whenever restoring an archive.

3.2.2.3 Advanced configuration through Director Management console

Basic configuration

The Director setup made in CLI mode (network parameters and communication protocols) is confirmed by viewing the "properties" in the GUI:



Domain Properties: Domain "dir"

Management Node Information

Name: dir

IP Address or Hostname: 10.4.192.21

Enable Password: *********** ☑ Save Password

Authentication Method

● SSH - Simple ○ SSH - RSA ○ Telnet

○ SSHv1 ● SSHv2

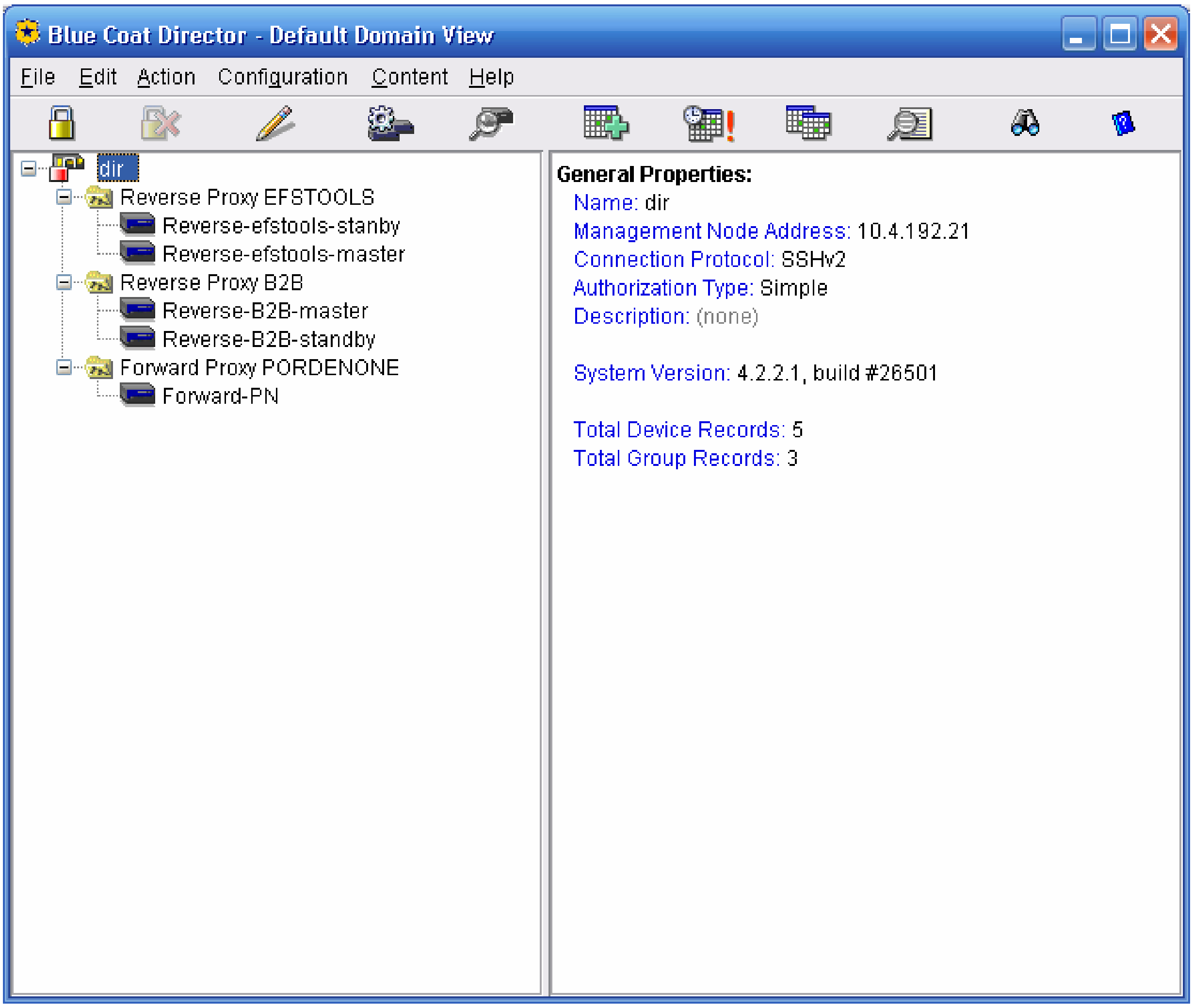
Simple Credentials

Username: admin

Password: ********** ☑ Save Password

Description

The Domain configured for Electrolux with the Management console is called “*dir*” and has all the Pordenone ProxySG appliances associated to it by proxy function; the Fig. 6 below shows the made setup:



General Properties:
Name: dir
Management Node Address: 10.4.192.21
Connection Protocol: SSHv2
Authorization Type: Simple
Description: (none)

System Version: 4.2.2.1, build #26501

Total Device Records: 5
Total Group Records: 3

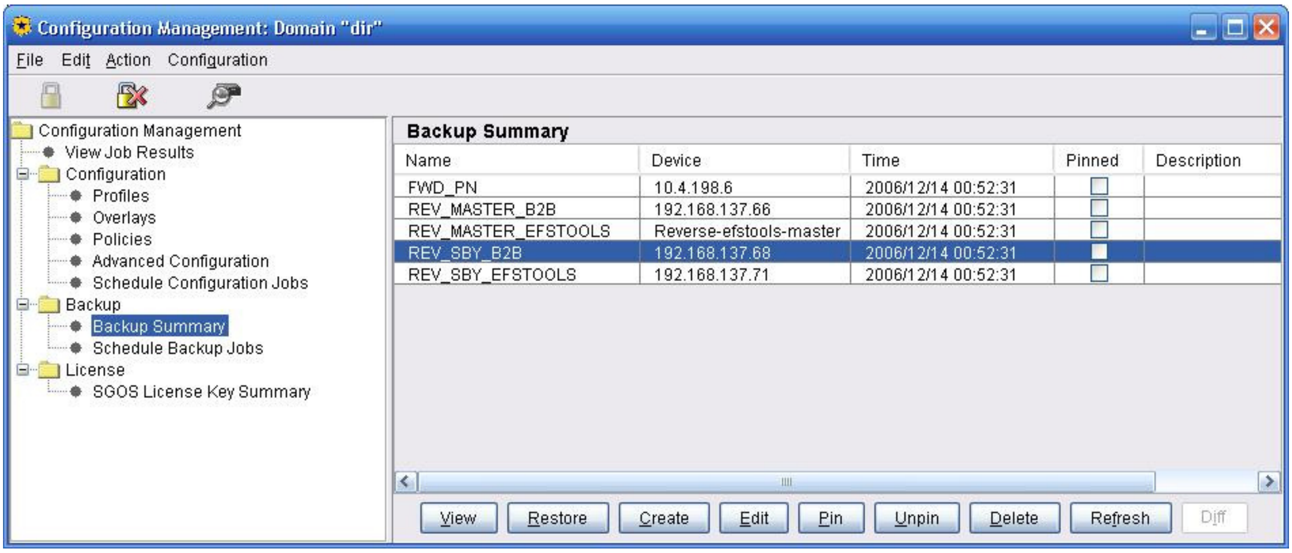
Fig. 6

The proxy IP address associated to the Director are summarized in the table below:

DESCRIPTION	IP ADDRESS
Reverse proxy “*B2B”* portal primary unit	192.168.137.66
Reverse proxy *“B2B”* portal backup unit	192.168.137.68
Reverse proxy *“professional sevices*” portal primary unit	192.168.137.70
Reverse proxy *“professional sevices*” portal backup unit	192.168.137.71
Forward proxy Electrolux Pordenone	10.4.198.6

ProxySG emergency Backups

After the successful communication between Director unit and ProxySG appliances a first backup was issued to archive on the management node, the actual production configurations loaded into proxies:

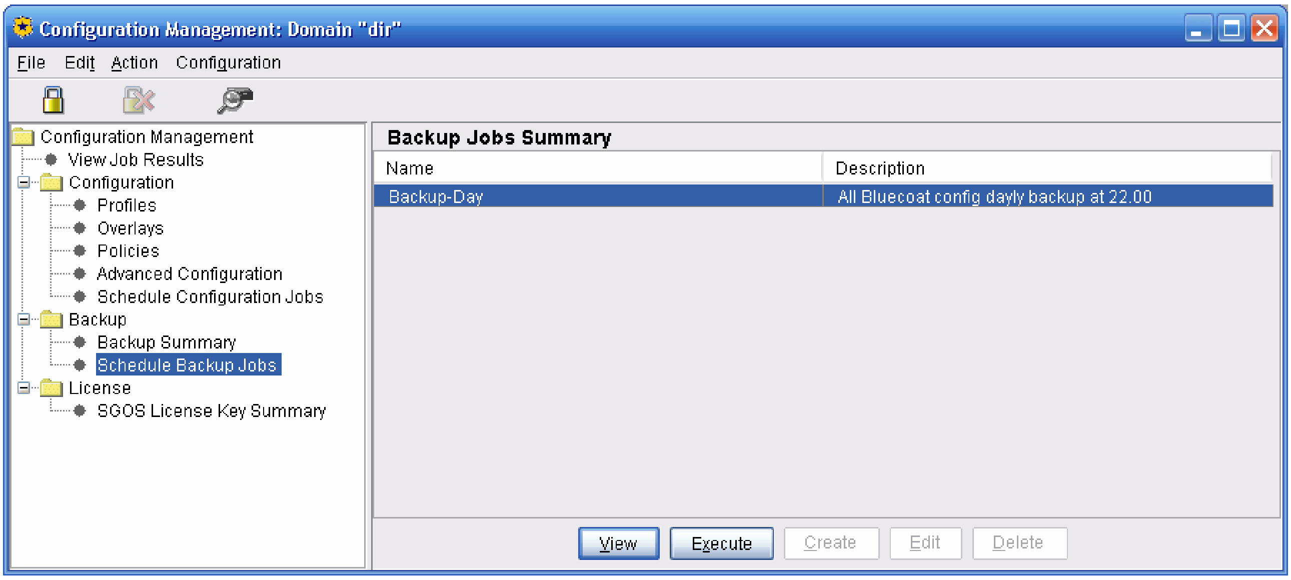


Backup Summary

Name	Device	Time	Pinned	Description
FWD_PN	10.4.198.6	2006/12/14 00:52:31	☐	
REV_MASTER_B2B	192.168.137.66	2006/12/14 00:52:31	☐	
REV_MASTER_EFSTOOLS	Reverse-efstools-master	2006/12/14 00:52:31	☐	
REV_SBY_B2B	192.168.137.68	2006/12/14 00:52:31	☐	
REV_SBY_EFSTOOLS	192.168.137.71	2006/12/14 00:52:31	☐	

Backup Job Scheduling

A Scheduled backup job was also configured to have a daily saving of all ProxySG appliance configurations; this was scheduled at 10pm Monday to Friday:



Backup Jobs Summary

Name	Description
Backup-Day	All Bluecoat config dayly backup at 22.00