Managed Services Technical Presentation
Service Provider Solution

Converged Managed Services
Delivery platform

Nov 08
Agenda

• About UBIqube

• Service Provider Solution Suite
  • Introduction, technology platform
  • Service delivery models

• Detailed Technical Services portfolio
  • Managed Router and Secure VPN
  • Managed Security (FW, IPS, Content Filtering)
  • Monitoring Alerting and Reporting
UBIqube is a global integrated network and security management solution vendor.

- France Telecom R&D Spin-off, incorporated in 2000
- Engineering in Grenoble, Sales presence in France, Russia, CIS, USA, Dubai and Hong Kong
- Innovative technology in the Management/OSS industry endorsed worldwide by bluechip leaders
<table>
<thead>
<tr>
<th>Technology</th>
<th>Management Segment</th>
<th>Market Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Device Monitoring</td>
<td>Lifecycle oriented solutions. (HPOV, etc.).</td>
</tr>
<tr>
<td>Vendor Specific CLI</td>
<td>Device Provisioning (Config MGNT / Change)</td>
<td>Mature segment. Costly.</td>
</tr>
</tbody>
</table>

**Converged Network & Security Management Solutions**
Addressing the Services Market Opportunity

The Winning Ingredients

• A Scalable, flexible and agnostic NOC/SOC
• An ecosystem of vendors and channel partners
• A sustained service oriented Marketing & Sales Strategy
UBIqube develops and markets 2 solution suites:

- **UBIqube Enterprise Solution Suite** helps organizations streamline their network and security lifecycle management.

- **UBIqube Service Provider Solution Suite** is the cornerstone of a Converged Managed Services offering.

These solutions are endorsed by the world leader of Network and Security equipment, Cisco.
About UBIqube

UBIqube Key differentiators:

- Simplicity
- Convergence
- Unified Solution
- Lifecycle Management

Brands and Logos: Cisco, Juniper, Fortinet, Blue Coat, Check Point, NetApp
Multi Tenant Web Based GUI

Reduces the level of expertise of field engineering in day to day routines.

Answers the branches proliferation (11% per year) management nightmare.

Value for the SP:
- Reduces the OPEX
- Offloads back office
- Reduces the delivery time

Value for the Customer:
- Reduces the costs (TCO and OPEX)

Pre defined Profiles
Multitenant Architecture
Role Based Access Control
VPN  FW  IPS  CF  Voice
ITIL Based
Service Delivery
KPI Monitoring  Alerting  SLA Management
Detailed Reporting  Compliancy  Log Management
Asset Management
Multiple CPE Vendors
Monitoring services
• Silver
• Gold
• Alerting
• Detailed Reports

Managed Voice
• CME/CUE
• UC500
• Dial Plan, Groups
• Self Care

Managed Security
• IPsec VPN
• Firewall
• IPS/IDS
• Content Filtering

Managed Router
• WAN / LAN accesses
• Network : DHCP, static routing
• NAT, QoS (co)
Service Provider Solution Suite

Differentiator: Lifecycle Management

- Networking
- Security
- VoiP
- Monitor and Respond
- Manage and Improve
- Deploy
- Test
- Reporting
- Monitoring
- Staging
- Provisioning
- Creation

11
Expand your Managed Service Portfolio and Addressable Market

Control your Cost Structure and Service Pricing
Service Provider Solution Suite

Solution Description

- Integrated Service Delivery Platform to deliver managed network and security services.

- Combining the MSActivator™ with UBIqube’s management appliance the SmartSOC-SA™ (Service Agent), provides a unique value proposition in the Managed Services industry.

- Features full service life cycle management from staging, provisioning, ITIL based configuration and asset management.

- Automation and predefined configuration profiles lower the cost of service delivery and reduce human error risk.

- The multi-tenant, web-based GUI called the VSOC simplifies service management in a multi-vendor and multi-technology environment.
Service Provider Solution Suite

Solution Modules

VSOC Webportal
- Unified GUI
- HTTPS

SEC Engine
- Staging
- Provisioning
- Management

Event Tracker
- Monitoring
- Alerting
- Reporting

Archive
- Backup
- Tamper Proof
- Archiving

PKI
- Authentication
- Automation

ITIL based CMDB
**Configuration management Database**

- Built on a set of oracle databases.
- ITIL compliant
- Handle all the configuration and all monitoring data.
- Dedicated databases store all the configuration information provided by the WEB Portal.
- Trigger the Sec Engine to update the managed devices.
- Another set of databases handle monitoring information.
- Provide logs and events storage and archiving.

**Oracle databases**
• **Event Tracker**
  - Logs and events collector
  - Handle syslog and flat files flows
  - A built in analysis engine provide logs classification and analysis
  - Load balance the events to a set of reporting engine
  - Upon the severity of the event, the engine triggers alerts.

• **C Language, Multi Threaded**
SEC Engine (Configuration Robot)

- Hide all the complexity of remote operation on a group of devices.
- Guarantee coherence of all the devices.
- Use a database of tested configuration fragments to calculate the new configuration for each device.
- Automatically update devices to allow dynamic Internet addresses configurations
- Propagate security updates.

C language, multi-threaded daemons
• **VSOC WEB portal**
  – Web-Based GUI: control your devices from anywhere.
  – High-level interface to administer one or many Edge devices.
  – Multi-Tenant architecture – with role based access control for service delegation

• Java based with Ajax on Tomcat and Apache Servers
The scope of a service provider is called an operator or VSOC (Virtual SOC).

The MSActivator supports different operators on the same physical SOC.

Customers are created inside one operator.

Security profiles are applied to managed device.

Devices and profiles are managed by the services providers called managers.
UBIqube Technology Platform

Role Based Access Control Concepts

Service Provider that need to manage only one operator

Service Provider Staff that can manage all or only a subset of customers. Or Customer with management capabilities

Privileged Administrator

Administrator A

Administrator B

UBIqube

Service Provider that need to manage several operators

Customer Read Only Console

Manager 1  
Manager 2

Customer A  
Customer B

Device 1

Device 2

Device 3

Profile 1

Profile 2

Operator AAA

Customer C  
Customer D

Device 1

Device 2

Profile 1

Operator BBB
Service Delivery Scenarios Overview

Service Provider Solution Suite

[Diagram of service delivery scenarios with labels and connections]
Service Provider Solution Suite

Service Delivery Scenarios

SmartSOC-SA

Local Log Archiving
LAN/DMZ Services
Legal Requirement

Central SOC Service Delivery
Off-Premises

Remote Service-Agent
On-Premises

Service Depth

MSActivator™

SmartSOC-SA
Service Delivery Scenarios – Centralized

ISP Backbone

Traffic Customer 1
Traffic Customer 2
Management
Service Delivery Scenarios – Service Agent

ISP #1
Lack of SP trust

ISP Backbone
Customer Network
SmartSOC Service Agent

ISP #1
ISP #2

Centralized SOC Management
Service Agent Management
Service Provider Solution Suite

Service Delivery Scenarios – Tiered

ISP #1

Service fulfillment
Config management
Event management

ISP Backbone

Customer Network

ISP #2

Integrator Service fulfillment partner

Service Provider Service Management

Integrator Service management

Customer Self-Service Reporting, Monitoring
• About UBIqube

• Service Provider Solution Suite
  ▪ Introduction, technology platform
  ▪ Service delivery models

• Detailed Technical Services portfolio
  ▪ Managed Router and Secure VPN
  ▪ Managed Security (FW, IPS, Content Filtering)
  ▪ Monitoring Alerting and Reporting
Managed VPN Services

Overview

- Managed IPsec VPN (PKI authentication)
  - LAN-2-LAN
  - Remote Access

- Managed Router (advanced)
  - Redundancy
  - QoS
• Transparent LAN-to-LAN connectivity
  – Normal routed network environment
  – Multiple subnets on each LAN

• Client-Server VPN or Mesh

• IPsec VPN featuring:
  – End-to-End Encryption
  – Authentication with Certificates
    • Avoids security risks with Pre-Shared Keys

• Dynamic Configuration Change Control
  – Automatic propagation of configuration Updates (eg new Device set up)
### Managed VPN Services

**LAN2LAN VPN**

<table>
<thead>
<tr>
<th>Device Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reachable</td>
<td>Device reachable but tunnel cannot be set up</td>
</tr>
<tr>
<td>reachable</td>
<td>Device reachable but tunnel does not work</td>
</tr>
<tr>
<td>unreachable</td>
<td>Device unreachable</td>
</tr>
<tr>
<td>error</td>
<td>Device not enabled</td>
</tr>
<tr>
<td>progress</td>
<td>Device in progress</td>
</tr>
<tr>
<td>backup device</td>
<td>Backup device in use but tunnel does not work</td>
</tr>
<tr>
<td>functions</td>
<td>VPN functions of the device disabled</td>
</tr>
<tr>
<td>functions</td>
<td>VPN functions of the peer disabled</td>
</tr>
<tr>
<td>unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>not tested</td>
<td>Not tested</td>
</tr>
</tbody>
</table>

**Sites and Locations**

- Fos Office e (INT293)
- Istanbul (INT210)
- Larnoune (INT1160)
- Moscow Office (INT1122)
Secure Remote Access for your Road Warriors
- Works with WiFi, UMTS... Usually “Just Works”
- LAN-like transparent connectivity to all the enterprise application

IPsec VPN featuring:
- End-to-End Encryption
- 2 phase Authentication with Certificates and Xauth
  - Avoids security risks with Pre-Shared Keys
  - Avoids security risks with Stolen Laptops
Managed VPN Services

Redundancy

- Double the Internet Access and routers
  - Protection against Failures
    - Of the equipment
    - Of the WAN link if a catastrophic failure occurs
  - Use two ADSL links from different ISPs
    - High Availability in actif / actif mode
  - Or Backup your MPLS VPN with ADSL VPN!

- Backup Broadband with Dial-Up
  - Poor substitute, but powerful recovery system
• Optimize the traffic on your access link, for example:
  – Define maximum bandwidth for Surfing
  – Define minimum bandwidth for Business Applications (VoIP)

• Modify your QoS policy to follow your network expansion
Managed VPN Services

QoS

Graphs showing network traffic data for different classes and protocols over time.
Managed Security Services

Overview

- Managed Security
  - Firewall
  - IDS/IPS
  - Anti-Virus
  - URL-Filtering
  - Anti-Spam
Managed Security Services

Firewall

- Firewall Security profiles
  - Configure one, deploy many

- Use of predefined recommended services
  - DNS, HTTP, POP, SMTP, IMAP ...

- 3 cookie cutters
  - Soho profile
  - Private DMZ profile
  - Public DMZ profile

- Reliable Remote Administration
  - No risk of being locked out from the router
Firewall Profiles

- Filter outgoing connections (inside/DMZ to outside)
- Filter communications inside the VPN (inside/DMZ to VPN)
- Control incoming connections (outside to inside/DMZ)
  - Port-Forwarding,
    - Allow incoming connections to Web and Mail servers
  - Static NAT
• **IDS/IPS profiles**
  – Configure one deploy many

• **Monitor suspicious behavior**
  – Globally or locally depending of interfaces

• **Signatures packs as cookie cutters**
  – Easy tuning of the IPS module

• **Automatic Signatures Updates**
  – Licence Warnings
  – False positive Management
Intrusion Detection Systems watch for anomalies
  – Requests without replies

Generates Alerts
  – Lots of Syslog messages
  – Needs centralized collection and presentation

Syslogs are stored in the SOC
  – Impossible for an attacker to hide the traces
  – Available for 1 month via vSOC
  – Post-mortem or Forensic analysis hides nothing
Managed Security Services

IPS/IDS

Daily Intrusion Prevention System Statistics

IPS - Top 5 Potential Attack Categories

<table>
<thead>
<tr>
<th>Attack Category</th>
<th>Inbound</th>
<th>Internal</th>
<th>Outbound</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

IPS - Top 5 Source Computers Sending Attacks

<table>
<thead>
<tr>
<th>Source Computer Sending Attacks</th>
<th>Flow</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.101.56.161</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.101.56.106</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.101.56.158</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.101.56.120</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPS - Top 5 Target Computers Receiving Attacks

<table>
<thead>
<tr>
<th>Target Computer Receiving Attacks</th>
<th>Flow</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.101.25.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.101.25.254</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPS Filtered Traffic - Hourly Activity

 Hour of the Day

15 16 17 18 19 20 21 22 23
• Critical business runs over the Internet
  – Viruses can be propagated over the Internet
  – Resulting in outages and lost revenue

• SecureDevice Anti Virus manages and monitors Anti-Virus on the Internet Gateway to guarantee:
  – Protection of internal network resources from virus attacks
  – E-mail and Web traffic Cleaning
  – Business continuity.
Managed Security Services

Anti-Virus

- Anti-Virus/Spyware profiles
  - Configure one, deploy many

- Monitor traffic
  - Globally or subsets of traffic (recommended services http, ftp, smtp, pop3 ...)

- 3 cookie cutters
  - Normal Anti Virus Profile (optimized performances)
  - High Anti Virus Profile (scan all files)
  - Paranoid Anti Virus Profile (scan all files recursively, update frequently, block all upon failure)

- Automatic Virus Databases Updates
  - Licence Warning
Anti-Spam

- To much spam in the inbox impacts employee productivity
- Prevent spam with very low false positives

Anti-Phishing

- Phising can lead to Identity company or personal credentials theft
- Prevent financial loss by adding protection against phishing attacks
Control Web Access
- Explicit or by type

Explicit declaration of URLs
- White-List or Black-List
  - Easy, but limited use

Restriction by type using a classification service
- Control employee Internet usage
- Block access to inappropriate or non-work-related WebDevices
- Improving employee productivity and limiting the risk of legal action
Managed Security Services

URL-Filtering
Managed Security Services

Vulnerability Assessment

- The embedded scanner scan devices for vulnerabilities
- The exploit database is automatically updated
- Can test managed or monitoring only devices
- Assessments can be schedules periodically
- Reports are available online on the Web Portal
Managed Security Services
Vulnerability Assessment

Profile Type: Scan vulnerabilities Profile
Security Profile Name: My first scan profile
Profile Comment: 

Scan days:
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

Hour to run the Scan on the devices: 12:50
Activated: 

Summary Overview

Vulnerabilities by security risks

Vulnerabilities by network services

- netbios-md (27/765)
- print (250/110)
- ms-sql (55/55)
- ms-nr (65/6)
- smtp (65/21)
- http (77/22)
- telnet (23/1)
- italk (225/25)
- mst-rpc (123/123)
- generic (120/120)
- netbios (200/200)
Profile based provisioning of:
- Telephony & Voice Mail configuration
- Data/Voice twin VLAN configuration on CME & UC routers
- SIP trunk configuration between CME & UC
- PSTN access configuration when FXO card available
- Simple VPN setup for non-VoIP routers (SOHO)
- Easy configuration of proper QoS settings for optimum VoIP experience
Managed Monitoring Services
Overview

- Silver Monitoring (SNMP)
  - Map view: Graphical Real-time Monitoring Console
  - KPI monitoring: Traffic, CPU load, Uptime, etc.
  - Threshold alerting

- Gold Monitoring (Syslog)
  - UBIscope and Security dashboard
  - Log analysis and alerting
  - Detailed Security PDF reports

- Asset Management
  - Software and hardware inventory
  - Licence management
Managed Monitoring Services

Real-time Console and MapView
Managed Monitoring Services

Real-time Console and MapView
Managed Monitoring Services

Silver Monitoring Network Statistics

• **Availability**
  - Real-time availability testing
  - After 6 consecutive failures, an alert is generated

• **Incoming/outgoing Traffic**
  - Monitor link saturation
  - Plan for QoS

• **Uptime**
  - Time since last reboot
  - Distinguish Network and Router problems

• **CPU Load**
  - Diagnose usage anomalies
  - Proactively propose upgrade
Managed Monitoring Services
Silver Monitoring Enhanced Statistics

- **Network Latency**
  - Monitor quality of ISP connection

- **IKE statistics**
  - VPN tunnels statistics
  - Identifies VPN module failures

- **QoS statistics**
  - Per traffic class statistics
  - Monitor forward and drop traffic

- **IPS statistics**
  - Monitor the number of IPS events
  - Sorted by Device or Profile
Managed Monitoring Services

Silver Monitoring Profiles

- KPI monitoring based on SNMP OID
- Custom graph rendering
- Threshold alerting
• **Security DashBoard**
  - Online alert reporting overview.
  - Event History per category
    - IPS, Firewall
    - Content Filtering
    - Logs
  - Top 5:
    - Device top 5 of the week/month: most attacked Devices
    - Alert top 5 of the week/month: the most frequent alerts
Log Analysis

- Compute weekly summary reports
- Aggregate the logs events on a per day basis
- Customize the logs with human readable information

Managed Monitoring Services

Gold Monitoring Log analysis
Alert Generation

- Discard the event (marked as false positive)
- Generate an email alerting

<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Severity</th>
<th>Description</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>17/11/2008</td>
<td>Firewall</td>
<td>Informational</td>
<td>SEC-6-IPACCESSLOGS / 0:0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17/11/2008</td>
<td>Syslog</td>
<td>Warning</td>
<td>VNOC-4-UNAVAIL / 0:0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17/11/2008</td>
<td>Firewall</td>
<td>Informational</td>
<td>SEC-6-IPACCESSLOGCP / 0:0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17/11/2008</td>
<td>Firewall</td>
<td>Informational</td>
<td>SEC-6-IPACCESSLOGDGP / 0:0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17/11/2008</td>
<td>Firewall</td>
<td>Informational</td>
<td>SEC-6-IPACCESSLOGRGL / 0:0 firewall event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17/11/2008</td>
<td>Syslog</td>
<td>Notice</td>
<td>SYS-5-CONFIG_1 / 0:0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Managed Monitoring Services
Gold Monitoring Detailed Reporting

• Daily and Monthly detailed Reports
Asset Management Services

Asset Management Inventory

- Updated and centralized software and hardware inventory reports
- Dynamically tracks all security assets managed without the need to schedule an audit
Asset Management Services
License Management

- Security modules licenses inventory
- Validity email alerting
Managed Monitoring Services

Gold Monitoring Auditing

• Configuration Backup
  – The running configuration of each device is downloaded and saved every night
  – Stored for 6 months
  – Locate illicit manual modifications

• Audit trail within UBIqube SOC
  – A record is retained of every modification
Managed, including monitoring and reporting

- **Cisco ISR Series** 800, 1800, 2800, 3800, 7200 ...
- **Cisco UC500 Series**
- **Cisco ASA Series** (CSC, AIP) 5505, 5510, 5520/40, 5550
- **Cisco PIX Series** 501, 506E, 515/525/535
- **Juniper ScreenOS Series** 5GT, ns25, 50, 204, 500
- **Juniper SSG** 5, 20, 140, 320, 520
- **Fortinet Fortigate** 60, 100, 200, 300, 400

Monitoring and Reporting

- Bluecoat SG
- Checkpoint Firewall 1
- Ironport – AsyncOS etc.
The market for Managed Services is a huge opportunity.

Telecom operators are well positioned to take advantage and generate margin intensive recurrent revenues while addressing customer churn, improve IT ops and walk the path of Value Added Service Provider.

Service Provider challenges are linked to Time-to-Service, Costs control, Service and routes to market definition, Sales&Marketing organisation.

Leveraging Cisco’s Service platforms together with UBIqube’s Service Delivery Platform allow to successfully address the Managed Service market opportunity