

## Regione Abruzzo is placing its trust in a Cisco Self-Defending network to bridge digital divide

Cisco end-to-end security is helping to enable the development of a wide range of advanced public services across Abruzzo, Italy

### EXECUTIVE SUMMARY

#### Customer Name

Regione Abruzzo – ARIT

#### Industry

Local Government

#### Location

Italy

Number of network nodes: 420

Number of ARIT employees: 50

Number of Regione Abruzzo employees: 1,800

Number of network users: 5,000

#### Business Challenge

- Bridge the digital divide in a region where access to IT is determined largely by geography
- Improve the efficiency and productivity of public services
- Remove information silos to stimulate a 'connected' approach to government and healthcare services

#### Network Solution

- Cisco's end-to-end approach to security, with a 'from-the-ground-up', Self-Defending Network architecture, has been the strategic objective in designing an IP-based regional network linking 420 sites with 24x7 management from a regional Security Operations Centre

#### Business Results

- A new generation of public services – from tax administration to healthcare – are being developed for citizens and businesses
- Capital and operating costs could be reduced through convergence and distributed intelligence throughout the network
- The economic and social imbalance between rural and urban areas is being addressed

### Business Challenge

Italy's Abruzzo region comprises 11,000 square kilometres dominated by the hills and mountains that stretch from the Apennines to the Adriatic Sea. It embraces the highest massifs of Central Italy, with landscapes of rugged beauty and peaks often higher than 2,000 metres.

It is a geography that shapes an area that many believe to be the heart of rustic Italy, but which today has created a digital divide. Most of the region's 1.3 million inhabitants live in the four county capitals, along the coast or in one of only a few dozen communities with over 10,000 people. The rest are scattered across the region in small villages, often inaccessible once the winter snow falls. Broadband connectivity is generally only available in the larger towns, while elsewhere services are limited to a sprinkling of ISDN lines, the PSTN and mobile phone access.

Vincenzo Consorti, Technical Director of ARIT (Agenzia Regionale per l'Informatica e la Telematica of Regione Abruzzo) – the publicly-owned agency responsible for the region's public sector information and communications technology (ICT) – explains the consequences of this imbalance. "ICT has become key to economic growth and we have seen a move of people from remote areas to the towns and coast where more advanced services are available. People will continue to live in small villages only if they are not 'left behind' in terms of access to information technology."

Regional government understood that ICT has the power to spur economic development and to improve public services and efficiencies. The team at ARIT also recognised that the existing regional network would not support the next generation of services needed to meet the region's social and economic objectives.

Unreliability and low bandwidth posed significant challenges to the region's ComNet-RA network – Community Network Regione Abruzzo – providing basic connectivity to 420 public sector sites, including local government offices, and hospitals.



**“Security is very often seen as something related to intrusion, authentication, antivirus software and so on. We were looking for much more than that. We needed to be sure that the network is protected and that the information we transfer over it will never be seen by someone who is not authorised to see it.”**

**–Vincenzo Consorti, Technical Director of ARIT- Agenzia Regionale per l’Informatica e la Telematica of Regione Abruzzo**

### Network Solution

In considering its plans to improve connectivity and bring more public services on-line, ARIT recognised that end-to-end security was of paramount importance.

“Connectivity by itself would not solve our problem,” says Vincenzo Consorti. “The most valuable applications tend to be those that carry the most sensitive, confidential information. We knew that people needed to be able to trust the security of the network because only if they trusted it would they use it.

“Security is very often seen as something related to intrusion, authentication, antivirus software and so on. We were looking for much more than that. We needed to be sure that the network is proactively and pervasively protected and that the information we transfer over it will never be seen by someone who is not authorised to see it,” explains Vincenzo Consorti.

In 2006, Regione Abruzzo, particularly the Struttura Speciale di Supporto Sistema Informativo Regionale (Special Unit Supporting Regional Information System), directed by Nello Ventresca, and ARIT, directed by Ernesto Esposito, started the project for its new secure, interconnected infrastructure – IIS-ComNet. Cisco’s vision of the Self-Defending Network and its distributed intelligence approach to security met all of ARIT’s requirements.

Cisco’s approach recognises that network security has evolved from independently deployed products such as firewalls to system-wide solutions. The transition to an information-driven global society both increases the value of information, and the need to control access to it. The Self-Defending Network helps maintain network availability and reliability. Rather than succumb to attack, networks must be able to absorb attacks and remain operational, much in the same way as the human immune system allows people to keep functioning in the presence of viruses and related bacterial infections.

“The excellence of Cisco’s approach and the breadth and depth of its security portfolio and technologies stood out. We believe that Cisco is the best supplier that could deliver a secure network of this scale. Point security solutions cannot work – only a holistic, fully integrated, collaborative and adaptive approach to security can deliver results in a real-world network,” says Vincenzo Consorti.

The carrier is providing wide area network connectivity – typically ADSL links at 2 Mbps – from the 420 sites back to the network’s main nodes at each of the region’s county capitals and to a data centre at L’Aquila, the regional capital.

The 420 sites are grouped into five categories depending on the number of users served. The groupings are:

- Main data processing infrastructure (Network Operating Centre, Security Operating Centre, Disaster Recovery, and so on)
- The four main nodes in the provincial capitals
- 337 sites, each with under 3,000 inhabitants
- 59 sites serving between 3,000 and 10,000 people
- 30 sites with over 10,000 inhabitants.

Depending on the size of the site, Cisco 2800 and 3800 Integrated Services Routers provide secure-WAN routing and advanced security features. A range of Cisco security solutions have been integrated at the SOC, which enable managers at ARIT's Security Operations Centre (SOC) to monitor and control every aspect of security throughout the network. Not only does the SOC give ARIT the ability to manage security, it also gives it the independence to negotiate connectivity in the future with different providers without the worry that changing a supplier of a managed security solution would bring.

**“The network will be both the catalyst and the enabler of a host of new services and ways of working that will touch many aspects of daily life throughout Abruzzo. This is only possible because the network inherently delivers end-to-end security.”**

**–Vincenzo Consorti, Technical Director of ARIT- Agenzia Regionale per l'Informatica e la Telematica of Regione Abruzzo**

### Business Results

The creation of a secure, highly available and flexible converged network is expected to transform public services across the region.

It is anticipated that secure access to information will help break down information silos, enabling a more coherent and holistic approach to services which can be designed around the citizen's needs rather than departmental objectives. Importantly, there are plans to provide citizens in the more remote parts of the region with access to these services, avoiding the need for difficult and time-consuming visits to council offices.

Business processes are being developed to provide feature-rich and more interactive services such as tax administration and land and building registries. As well as helping to improve efficiency and thereby increasing departmental productivity, other cost-savings are likely to come from a web-enabled approach to areas such as office supplies ordering and replenishment through economies of scale.

The region's economy could also benefit from a series of initiatives ranging from helping to boost tourism in an area of outstanding natural beauty, to supporting marketing initiatives such as the official classification of locally produced food and wine which are important regional assets.

In addition, the network is expected to play a major role in improving healthcare across the region. As well as helping to enable a variety of time-saving and convenient administrative services, such as hospital and out-patient appointments to be put on-line, the network could enable better utilisation of scarce medical resources and expertise. Telemedicine could make for faster diagnoses, with remote access to hospital-based medical specialists and tools. Healthcare administration across the region could also greatly benefit from better data integration and systems able to monitor and consolidate key metrics such as expenses, inventories and levels of service.

“The network will be both the catalyst and the enabler of a host of new services and ways of working that will touch many aspects of daily life throughout Abruzzo,” explains Vincenzo Consorti. “This is only possible because the network delivers end-to-end security.”

Convergence can also deliver a range of future benefits including the ability to introduce Unified Communications, with voice and messaging on the same multiservice, Self-Defending Network platform. This could dramatically cut operating costs by removing the need to maintain and manage a separate voice infrastructure, and also by simplifying telephony ‘adds, moves and changes.’ Call charges between departments and offices could also dramatically reduce as traffic is kept on the network and not carried over the public switched telephone network (PSTN).

## Technical Blueprint

The Cisco Integrated Services Routers are optimised with specially designed hardware architecture that delivers high performance and sophisticated security features such as VPN support, built-in accelerated encryption, firewalling and inline Intrusion Prevention services. Additionally, this family of routers is able to support other advanced services such as Cisco Unified Communications – including IP Telephony – and wireless networking

A Cisco Security Management Suite, including the Cisco Security Manager (CSM) and the Cisco Security Monitoring, Analysis, and Response System (MARS) is at the heart of the Region's new SOC. It provides the framework for next-generation security management tools designed for the operational management and policy administration of the Cisco Self-Defending Network.

This suite of integrated and collaborative applications simplifies the management process by automating tasks associated with the functional areas of security management: configuration, monitoring, analysis, mitigation, identity and auditing. Security related events from devices anywhere within the network are automatically forwarded to the SOC where they are analyzed by the Cisco Security Management Suite and presented to network managers along with suggested actions for resolution and mitigation based on best practice.

A Cisco Secure Access Control Server Engine can extend access security by combining authentication, user or administrator access, and policy control from the centralised identity-based networking framework. This can give greater flexibility, mobility, and security, which can result in user productivity gains.

Powerful protection against virus, spam and phishing is provided by the Cisco Adaptive Security Appliances (ASA 5500 Series) which look deep into data packets through its integrated Content Security Control Security Services Module (CSC-SSM) and its associated Application Layer Anti-X protection features. These appliances also support Cisco Intrusion Protection System (IPS) to assess and react to threats, delivering enhanced network scalability and resiliency. These ubiquitous security services, across any part and node of the network, include cross-solution feedback linkages, common policy management, multi-vendor event correlation, attack path identification, passive/active fingerprinting, and host-based (Cisco Security Agent) IPS collaboration.

## Next Steps

The roll-out of the network is on track for completion by 2008. Designed as a secure and flexible platform for converged services, the team at ARIT is already developing plans to deploy Unified Communications – including IP Telephony – over this Self-Defending Network, leveraging the powerful and sophisticated V<sup>3</sup>PN (Voice and Video over VPN) functionality across its WAN connections. End-to-end Quality of Service (QoS) also opens up the possibility to introduce video-based services such as Cisco TelePresence, which would be of particular benefit in such a mountainous region as Abruzzo.

## For More Information

To find out more about Cisco Security solutions, go to: [www.cisco.com/go/selfdefend](http://www.cisco.com/go/selfdefend) and [www.cisco.com/go/security](http://www.cisco.com/go/security)

### PRODUCT LIST

Cisco networking and security services, including:

- Cisco Integrated Services Router 3800 and 2800 series equipped with Security bundles: <http://www.cisco.com/go/isr>
- Cisco Adaptive Security Appliance 5500 Series Anti-X Edition: <http://www.ciso.com/go/asa>
- Cisco Security Manager (CSM): <http://www.cisco.com/go/csm>
- Cisco Security Monitoring, Analysis, Response System (CS-MARS): <http://www.cisco.com/go/mars>
- Cisco Secure Access Control Server Engine (ACS): <http://www.cisco.com/go/acs>
- CiscoWorks LAN Manager Solution



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0800 020 0791  
Fax: +31 020 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo and the Cisco Square Bridge logo are trademarks of Cisco Systems Inc.; Changing the Way We Work, Live, Play, and Learn, is a service mark of Cisco Systems Inc; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.