WHITE PAPER

ATLAS i60 - CLOUD EDGE ROUTER

TELDAT PROPOSAL FOR THE ENTERPRISE BRANCH OFFICE ACCESS ROUTER IN THE CLOUD COMPUTING WORLD

Revision: 1.3 November 25, 2012

TABLE OF CONTENTS

1. Introduction

This document describes Teldat proposal for the enterprise branch office access router in a moment in which the IT and enterprise communications are undertaking a deep shift in paradigm. Technology has made possible new ways to face the business needs regarding IT and communications and the advantages it entails are speeding up the widespread adoption of new applications and services derived out of the new technologies.

In this dynamic world, the enterprise branch office will also see big changes. Teldat proposes an innovative but safe path for the evolution of the branch office access router, so that corporations and telecom operators can answer these new challenges with confidence and flexibility in a rapid changing environment.

As this whitepaper will describe in detail, Teldat new enterprise access router flagship, the Atlas i60, is not "yet another router" on Teldat portfolio, but a new concept grouping a modular branch office access router with outstanding performance, an integrated LAN switch, an embedded Linux-based applications server, a wide family of applications for such server and a cloud-based Software-as-a-Service (SaaS) platform for the professional-grade standards-based management of such a complete proposal.

2. Challenges of the Cloud Computing paradigm for the enterprise branch office access router

From its early days of the X.25 line multiplexers to nowadays high-speed metro Ethernet access routers, the enterprise branch office access router has always had a common purpose: to provide communication services to the IT infrastructure and applications serving the branch office.

Nevertheless, the features or services required for such mandate have varied throughout the years, depending on the technology and/or carrier service in place: throughput, security, management, etc.

Several IT paradigms have shaped the communications landscape in this last 30-40 years, both because and as a consequence of the available communications services to the business operations of enterprises and corporations: mainframes, client-server, Internet.

Today is no exception. On the contrary, we are in the dawn of a big shift in this paradigm.

Several key factors are affecting the way enterprises plan and deploy their communications networks:

- The cloud computing model
- The broadband phenomenon
- The mobility
- The outsourcing business model

2.1. The cloud computing model

Server virtualization led to data center consolidation and data center consolidation led to the cloud computing paradigm.

Today, cloud computing is well established in the residential market, with new applications and services like Dropbox, Google docs or Apple's iCloud. The number of corporations using cloud services to implement their business applications is still scarce, but the industry consensus[1] is that considerable adoption is inevitable and that is finally taking off; being it based on a public cloud, a private cloud or hybrid.

[1] See Enterprise Q1 2012 Survey from Strategy Analytics, Inc.

Figure 1: Different cloud PaaS providers.

The migration of the enterprise IT systems to the cloud is not free of concerns for the IT managers[2]: security, availability, performance, payment model, interoperability, back to in-house model, difficulty to integrate and ability to customize are the major concerns of IT managers analyzing the cloud adoption.

But, what are the implications of the cloud computing adoption on the enterprise for the branch office access router? Is not it contradictory to deploy a "smarter" access router when the cloud computing model moves all the intelligence to the "cloud"? A quick answer could suggest that those two concepts, cloud and a smarter access router, are contradictory, but a more careful analysis, as we will perform throughout this white paper, indicates that there is in fact room for both ideas, becoming "complementary" concepts that reinforce each other when adequately used:

- Cloud computing introduces new needs on the WAN communications and on the infrastructure to be deployed at the customer premises: security, WAN optimization, etc. In this white paper, we will see several examples of applications that address those new needs and that it makes sense to integrate or embed in the access router.
- Not everything or every application is adequate to be virtualized and moved to the cloud, either for technical or economic reasons. For instance, an USB port, or better, the USB device to be connected, such as a webcam, would be too expensive to virtualize: raw USB data to be transmitted to the network to be processed (decoded, etc.) in the cloud does not pay off. But if you have moved all your local servers to the cloud, where can you connect this USB device?
- Once you have a smarter access router, the corporations can use it to efficiently deploy a wide range of other business applications that otherwise would have to be delivered with external servers or appliances.
- The cloud computing adoption for the enterprise business applications can be accomplished more securely when the branch office has "extra" power to interact or complement the cloud services. Those fears of the cloud computing model mentioned above can be smoothened or reduced if the IT manager has an ally on the branch office. Flexibility and time to market can also be improved when the cloud services have a smart "point-of-presence" at the customer premises they can rely on.

The integration of this new applications and services with the cloud and so the integration of the access routers where they can now be executed, is not mandatory: some applications can be completely independent of a cloud service. But, since the cloud is going to be there no matter what and the access router is also going to be a sure thing on the equation, the more they interact and complement each other, the more value they can "capture" out of the

[2] See IDC Enterprise panel 3Q09

branch office value chain, to provide competitive advantage or cost savings to the corporations using them.

2.2. The broadband phenomenon

The Internet access residential market is driving a lot of investment and innovation on the access equipment supply chain: IC vendors, middleware providers and device manufacturers dedicate a lot of resources to cope with the demand of new added value devices with even higher performance and features than a traditional SMB access router. In the past, it used to be the opposite, where technologies and ideas developed for the enterprise market on a first stage were adopted by the residential market on a later stage.

Carriers are also struggling to differentiate and monetize that difference, competing with each other and with Over-the-Top (OTT) providers that rely on the broadband infrastructure but do not have to invest on it: Skype, Google, Apple, etc. are capturing the value of the customer applications using the "dumb pipes" provided by the telecom players.

This broadband phenomenon is both a driver and a need for the cloud computing model described previously.

But, what are the consequences of this broadband availability for the enterprise branch office?

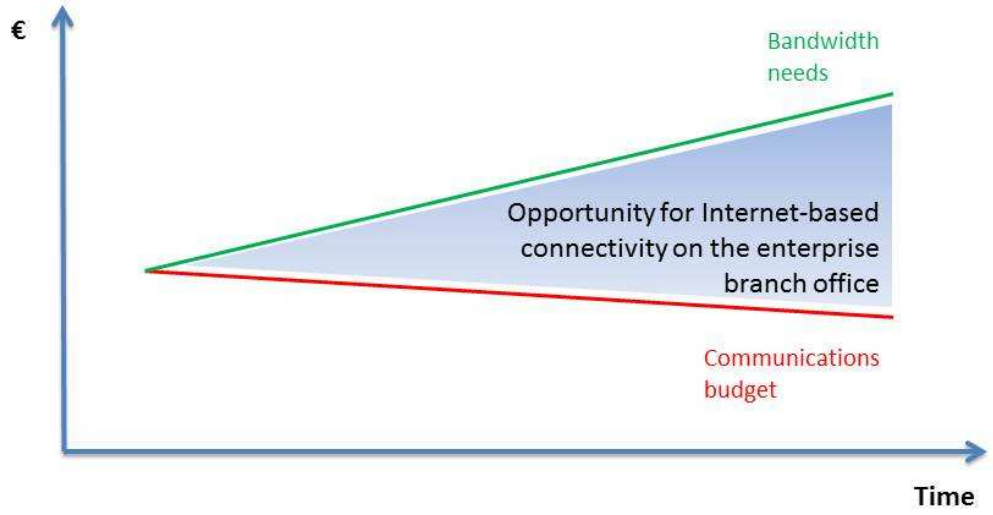

Figure 2: Opportunity for Internet-based connectivity on the enterprise branch office.

As Figure 2 shows, since the expected evolution of the communications budget (in price per Mbps) of the enterprise branch office, normally MPLS-based, will not be able to cope with the data communications needs in the foreseen future, there is a clear need for "cheaper" bandwidth to fill this gap. And here is where the broadband technologies being used on the residential market can offer a very convenient solution, if not as a full replacement of existing MPLS services, which the carriers are "milking", at least for the overflow of certain non-critical traffic or for backup of the existing enterprise-grade service.

The use of direct residential-grade Internet connections on the enterprise branch office will open new opportunities for smarter access routers and associated cloud-based services to handle the characteristics of this new "nonprofessional-gade" communications environment: security, WAN optimization, load balancing/aggregation, etc.

2.3. The mobility

Another market trend with origin on the residential/consumer market, that is also reshaping the enterprise market, is the mobility. Mobile operators' investment efforts are being directed mostly to deploy or extend the infrastructure to provide 3G/4G services to the residential users.

But these mainstream services and their associated devices are also being used in the enterprise world. The BYOD (Bring Your Own Device) trend, in which the employees of an enterprise or corporation bring their own smartphones and tablets to the office, is making use of the mobile terminals and services design for the residential market, creating at the same time new threats (and opportunities) for the enterprise. The trend is actually happening; so the IT managers should rather prepare to manage it and try to integrate it into the organization business operations than trying to fight it. This is creating new needs in security, authentication, information management, etc.

But how does this trend affect the enterprise branch office access router? There are at least two different facets of this trend to be considered:

- **3G/4G residential services will be widely available**. Mobile carriers' business models and future profitability will depend very much on their ability to monetize the mobile data stream[3]. This will make them be cautious about the mobile data business proposal to the market and probably will eliminate flat fee schemes, as we have already started to see. Nevertheless, the close-to-universal coverage will be there, the services will be there and the enterprises will be able to use them to a great extent. The LTE bandwidth is "good enough" for many enterprise branch offices, if not as the only WAN connectivity of the branch office at least for backup, in case of failure on the main link, or to overflow part of the branch office traffic.
- **Mobile terminal diversity and loss of PC supremacy**. The BYOD trend, the increased diversity on the number and type of terminals and operating systems (PC alternatives) and the dynamic nature of this fast evolving market are other good reasons to add "intelligence" to the enterprise branch office. As we will see on this white paper, the Atlas i60, with the possibility to execute a wide range of applications, offers a good support to manage all this new complexity: security applications such as wireless IDS, management applications such as inventory and IP address management are just a few applications that can help the IT managers to survive in this new dynamic world.

3. Atlas i60 value proposition

After having analyzed the key factors that will challenge the enterprise branch office access router in the short to mid-term future, what is Teldat proposing to response to those challenges and needs?

[3] See Arthur D. Lite's March 2012 Telecom Operators "Let's face it" report, page 28 ("Sensitivity analysis: mobile data the largest uncertainty")

3.1. The value proposition

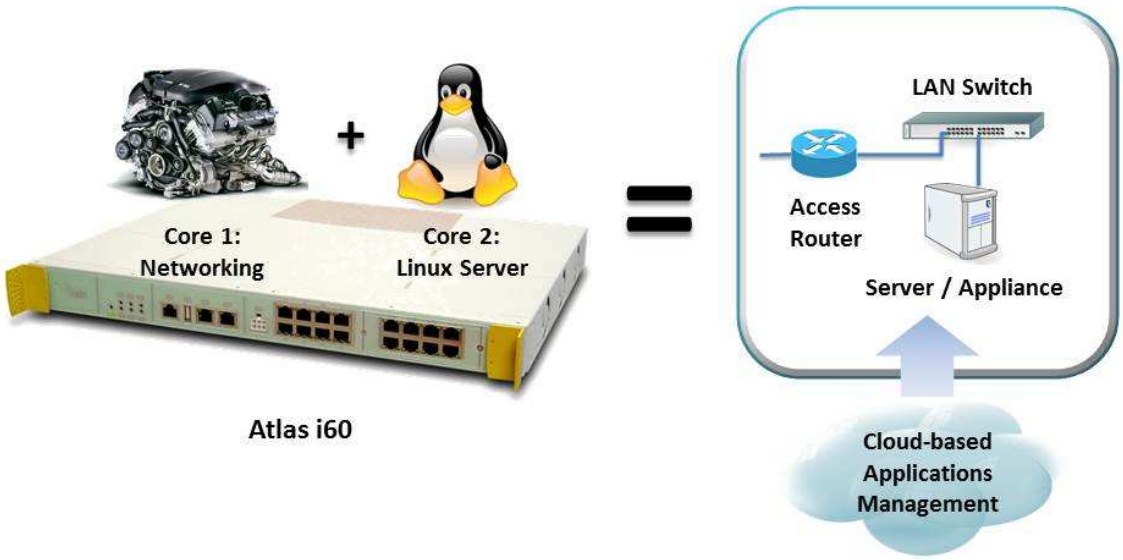

Figure 3: Atlas i60 value proposition.

As Figure 3 shows, Teldat proposes the use of its Atlas i60 enterprise branch office access router, which also embeds an open Linux server, that together conform a "Cloud Edge Router" in which the customer can run applications. These applications can be developed by Teldat, by third parties or by the customer itself, offering a really open platform with no lock-in threats for the customer.

This "Cloud Edge Router" is complemented with a cloud-based services platform to manage the applications that run on the embedded Linux server. This cloud service, which can also be alternatively provided as a traditional management console for big corporate customers to integrate on their own private clouds or data centers, will be described later in section 4: "Teldat cloud-based services platform".

In summary, Teldat proposal is made up of five components integrated into a single system:

- **Enterprise-grade professional access router**. See Annex 1 for a summary of the Atlas i60 networking features.
- **Embedded managed LAN switch** with optional POE.
- **Embedded Linux server/appliance**. Allows for the execution of applications, independently of and without affecting or being affected by the communications side of the access router. The Atlas i60 is powered by a dual-core CPU. Teldat Networking software stack (CIT) runs in one of the cores. The embedded Linux server runs in the other core. This offers a cost-effective implementation of two different systems into a single device, sharing common costs, such as housing, power supply or memory (although logically each core uses a separate part of the memory for secure and independent operation).
- **The applications** themselves, to be executed on the Linux server.
- **Cloud-based SaaS management service** for the embedded applications life-cycle management. This service will also be extended progressively to offer centralized management of the applications themselves. For instance, a centralized content manager plug-in for the Teldat cloud-service will offer a cloud-based console for the management of the remote Digital Signage applications that run on the Atlas i60 access routers. From this "plug-in" cloud-based service, the customers will be able to

generate the multimedia content, the programing grids and the update policy as well as the monitoring of the remote Digital Signage applications running on the Atlas i60 access routers.

3.2. Applications positioning

Is all this worth it? What applications does it make sense to execute on the access router?

The Atlas i60 CPU, although very powerful for an enterprise branch office access router, as can be seen in the performance comparison charts in Annex 1, cannot compete in performance with the CPUs of today's dedicated servers and appliances. On the other hand, there are many applications for which a dedicated server is over-dimensioned, at least for the required performance in a typical branch office. For this type of applications, the Atlas i60 has no match in price/performance ratio.

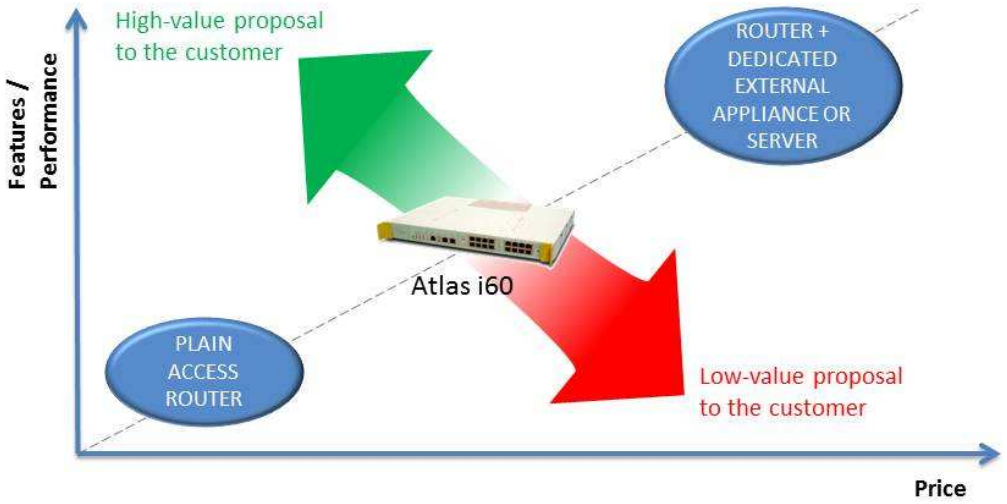

Figure 4: Atlas i60 applications positioning.

Figure 4 shows this positioning for the Atlas i60 applications. On the left side of the picture, the "traditional" branch office data communications equipment will consist basically on the access router alone. Some enterprise-grade access routers are starting to incorporate features such as advanced firewalling, IDS, anti-virus, etc. But normally, if those features are enabled, the routing performance drops drastically. This occurs because those features share the CPU and software stack with the networking routing and the CPU is not dimensioned to support these extra features. This configuration has the lowest price of all, but also the lowest performance or features. On the right side of the picture, a more demanding branch office will include not only the access router but also a dedicated external server or appliance for a specific application. You could also have more than one appliance for several applications. This configuration is the most expensive of all, but also the one that offers more performance or features. And you can always scale up with a more powerful and expensive appliance. This is the only solution available if the branch office "really" needs the features or performance provided by the external appliance.

But there is a gap in the middle of the picture that can only be filled with the Atlas i60:

- The "standard" access routers cannot scale up in performance and are also closed systems where generic applications cannot be run.

- The external appliances or servers do not scale down well, since normally the cheapest appliance of a given vendor is too expensive for the small-medium branch office, with prices typically one order of magnitude bigger than the price of the access router.

This analysis is generic and applicable to all types of applications, not only the security applications mentioned above. For instance, a Digital Signage application, WAN optimization applications, management probes or applications, etc. All of them can generically run on external appliances or servers, but can also run on the Atlas i60, with reduced performance in general, but for a fraction of the cost of the external appliance or server.

Per-application and per-customer analysis is required to understand if the Atlas i60 is suitable for a specific application on a specific customer. It will depend on each customer requirements and the CPU power and memory size required to meet those specific requirements. For instance, the serving throughput required on the LAN of a web cache application may be different for different customers; and the CPU and memory requirements of an inventory application are different from the requirements of office automation application.

Figure 5 illustrates a very simplified version of the proposed evolution of the enterprise branch office access router with the Atlas i60. For simplicity, many elements of a real branch office and central premises infrastructure have been removed, like printers and many secondary elements for the purposes of the topic being illustrated. Also, for clarity, the picture does not show other key elements, such as the voice infrastructure and backup or redundant communications lines, for which the Atlas i60 can play an important role as it will be shown briefly in this white paper. But, as the picture shows, the Atlas i60 allows for a future-proof migration of the branch office communications infrastructure in the cloud computing world.

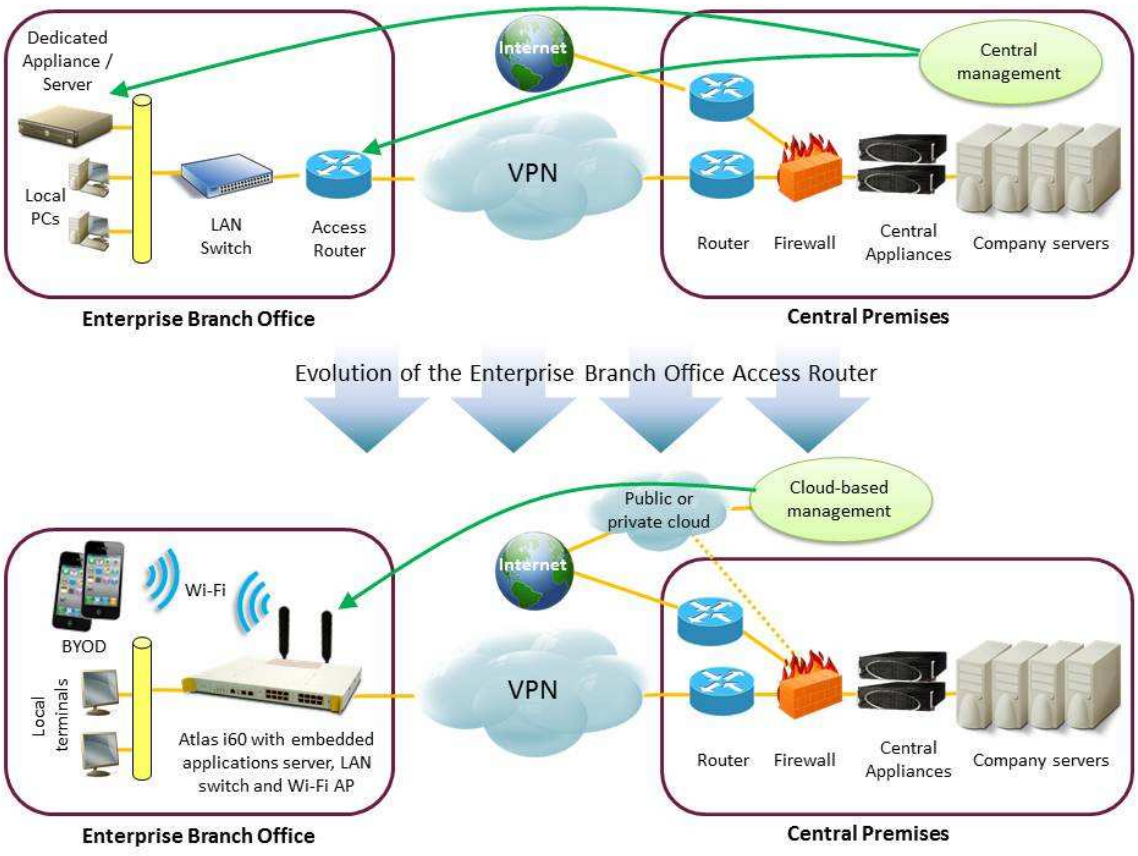

Figure 5: Evolution of the Enterprise Branch Office Access Router.

3.3. Advantages

The main advantages of Teldat proposal are:

- **Cost-effective**. The total cost of ownership that the Atlas i60 allows for is considerable less than alternative solutions, as explained in Figure 4. This advantage is true for the initial investment of the equipment or CAPEX but it is even bigger considering the OPEX or management and operation costs throughout the life of the equipment. Teldat implementation of this concept very much helps to keep the prices low, since as it was described in section 3.1, the use of a dual core CPU is less expensive than the use a dedicated server or appliance or, as other vendors propose, the use of an embedded PC in the access router chassis.
- **No lock-in effect**. Teldat proposal is open and based on standards. It uses a standard Linux distribution on the embedded server of the router. It also uses a public cloud service and, whenever possible, standard-based procedures on the cloud operation (REST). The cloud service is based on APIs and can be easily moved to other cloud platforms, public or private. This way, the customers can be confident with the adoption of our proposal.
- **Openness**. One sample of the no lock-in effect commented above is the fact that the customers can easily port their own-developed applications into the Atlas i60 platform if they choose so. All the tools of the Linux Debian distribution are available for them to create or port their own applications: toolchain, packing system, etc. This offers a secure and flexible evolution path, to answer the challenges of the ever-changing IT environment.
- **Flexibility**. The use of a standard Linux distribution allows for potential licensing of third party software. It will be up to those third parties to collaborate or not, if needed, but at least Teldat offers a standard platform that will eliminate or heavily reduce technical difficulties of such licensing, paving the way for a quick integration.
- **Seamless management**. Teldat has more than 25 years of experience offering communications products for enterprises and corporations. Teldat knows that the management is a key element for this market. Big corporations and many times the telecom operators serving them, with thousands of remote branch offices to interconnect, need a professional-grade management solution for the communications infrastructure. In the cloud computing era and with the proposal that Teldat is making, this is true more than ever. Although integrated into a single system, the embedded applications add another level of complexity that has to be managed. Similarly to the differences between a regular mobile phone and a smartphone, where the smartphone can incorporate numerous applications that the user need to manage (buy, install, uninstall, etc.) the Atlas i60, in comparison with a standard “plain-old-router”, supports embedded applications that need to be managed. As an example, a clear situation well-known to IT managers: when an Atlas i60 serving a branch office breaks down and has to be replace, the replacement, normally under a NBD (Next Business Day) or 8x5x4 (Next 4 working hours) outsourced maintenance service, has to be simple and automated, but the operator replacing the router does not perform complex configuration tasks. This has to be true even if the Atlas i60 has different applications embedded. Teldat proposal for this seamless management is described in section 4, “Teldat cloud-based services platform”.
- **Independent of the communications stack**. Since the Linux server runs on one of the CPU cores, independently of the networking stack (CIT) that runs on the other core, the load of each core (usage of the core) does not affect the other one. So, the routing performance of the Atlas i60, as a router, is not affected by the applications run in the Linux server side and vice versa. A more detail explanation on the Atlas i60 architecture and cores intercommunication is described in Annex 2.

3.4. Specific value proposition for vertical markets

The Atlas i60 access router is the first member of Teldat product line to support the innovative concept that is described in this white paper. But it will not be the only one. Teldat has planned or under development specific value propositions for vertical markets such as Financial Entities, In-vehicle applications or Utilities, which will also include this concept.

4. Teldat cloud-based services platform

4.1. Teldat public-cloud "Services Platform" SaaS

As previously introduced in section 3.1, "The value proposition", Teldat wraps the equipment part of the proposal with a cloud-based services platform. Figure 6 illustrates this concept.

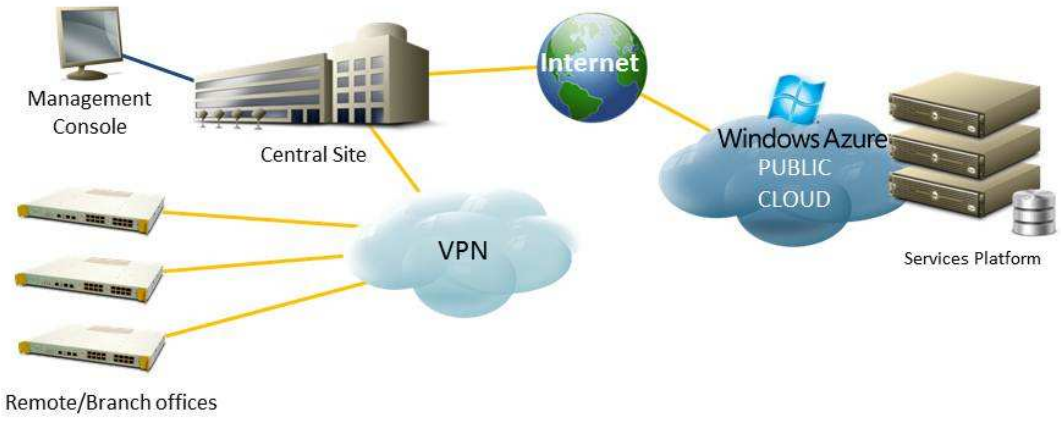

Figure 6: Teldat public-cloud "Services Platform" SaaS.

The main functionality of this services platform is to manage the life cycle of the applications that run on the deployed Atlas i60 access routers or, in other words, to provide a centralized way to install, uninstall, upgrade, start, stop, restart, etc. different applications, of different customers, on their corresponding Atlas i60 access routers. If the networking side of the access router is typically managed from a centralized server that configures and monitors those remote access routers, the applications side of the Atlas i60 is managed from a cloud-based service that allows for the installation, execution, etc. of the applications.

The second functionality of this "services platform" is to provide a unified, standards-based, foundation to (1) integrate the management of the remote applications themselves into the same cloud-service and to (2) implement the central servers for applications that require them. The first functionality of the "services platform" allows for the centralized installation of any application on the remote Atlas i60 routers, for instance a Digital Signage application. The second functionality allows for the centralized configuration and monitoring of each one of the remote Digital Signage instances and for the execution of the central "content server" of the Digital Signage service, which generates the multimedia content and the programming grid for each of the remote instances (see Figure 25).

This "Services Platform" for the Atlas i60 is a key element of the proposal, which would not work without it, since big deployments, as typically those of the corporate and enterprise market, can only be possible when properly managed. Teldat has applied its extensive experience as a network manufacturer to provide a professional, business-grade management platform to handle the added complexity that the applications introduce and offer an operative experience as rich as possible, keeping the management of communications side as close as possible to today's experience.

4.2. Applications life-cycle management

The applications life-cycle management side of the Services Platform has itself two main features, application synchronization and data backup. The application synchronization feature is shown in Figure 7. It is used to manage which application has to be loaded on each remote router. It keeps a centralized repository of applications and a database to control where those applications have to be installed. As mentioned, it allows installing, uninstalling, starting or stopping applications on the remote routers. The data backup feature is shown in Figure 8. It is an optional feature for each application, which copies the application data into the cloud, for a later restoral, if needed.

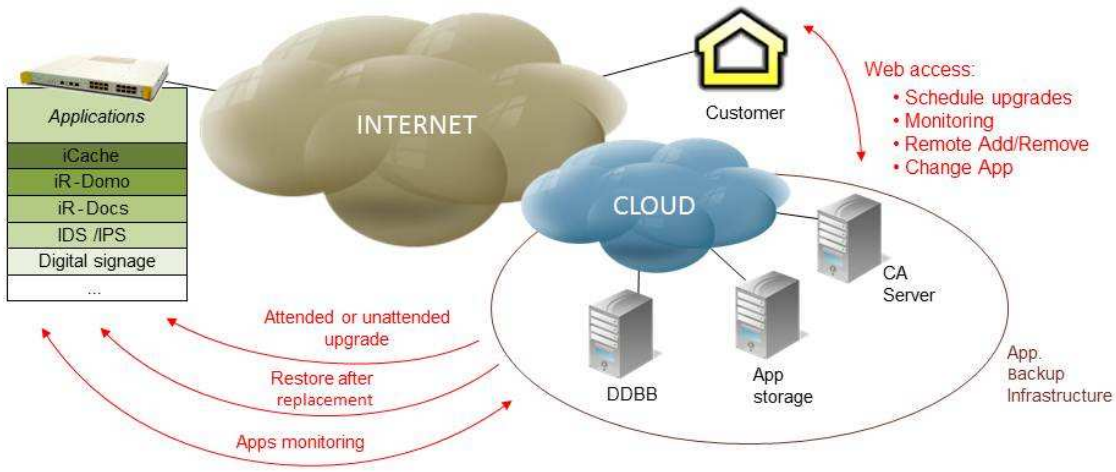

Figure 7: Application synchronization feature of the cloud-based Services Platform.

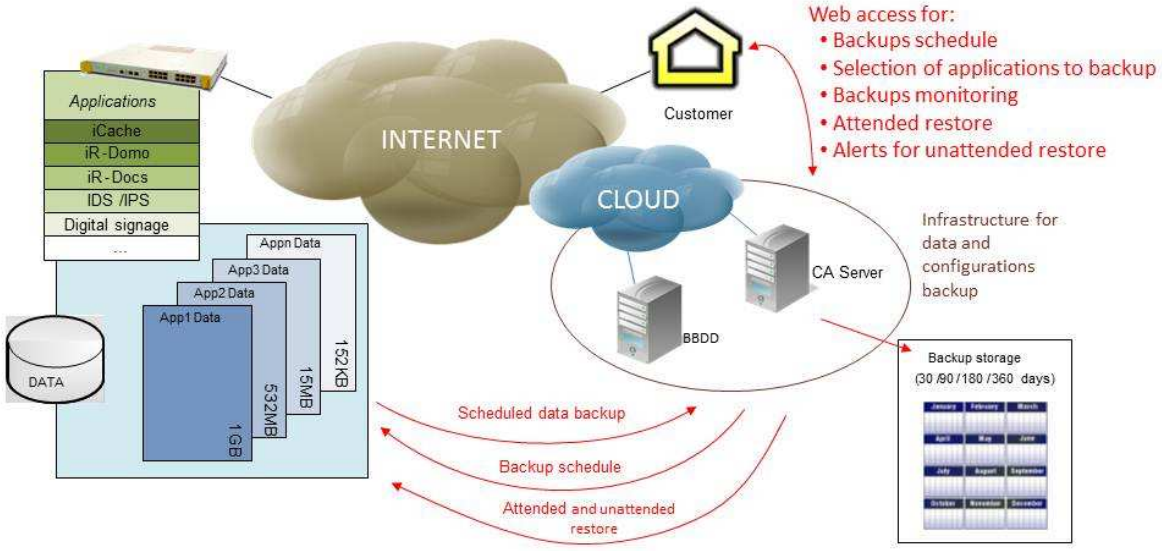

Figure 8: Data backup feature of the cloud-based Services Platform.

4.3. Teldat SaaS advantages

The main advantages of this cloud-based Services Platform are:

- **Fast time-to-market**. It offers a ready-to-use, complete out-of-the-box turn-key solution.
- **Independent of the networking side**. It offers a management solution for the applications that is independent and compatible with the management of the communications side on the routers, for an easy installation or replacement of devices. Thus, applications and networking management can be offer by the same entity or by different ones.
- **Advantages related to the "cloud"**. Since it is a cloud-based service (SaaS) it offers the advantages associated with this type of IT implementation: efficiency, security, resilience, scalability, etc.
- **Implementation flexibility**. By default, Teldat offers this service in a public cloud (Microsoft Azure), but because of its internal modularity and because it has been design from scratch with this feature in mind, it can be easily adapted to another public or private cloud. So, it is prepared to interface with multiple public cloud services.
- **Extensibility**. As described above, the Services Platform can be "extended" with "plug-ins" to support the management of each of the applications (control the functionality of each of the applications from the same cloud service) or to implement central servers that some of those applications may require.
- **Security**. The applications life cycle management is protected by digital certificates and each application has to be signed in order to be accepted.
- **Ubiquitous web user interface**.

Finally, as briefly mentioned in section 3.1, this cloud service can also be provided as a traditional management console for big corporate customers to integrate on their own private clouds or data centers. In this case, Teldat offer the software and it is the customer's responsibility to install, maintain and operate that service.

5. Applications catalog

The applications are Teldat key component of the proposal for the Enterprise Branch Office Access Router. After the justification for the advantages of embedding applications on the access router in certain cases, as described in section 3.2, this chapter introduces a catalog of applications that Teldat has developed[4].

[4] Some of the applications described here, at the time of writing this white paper, are still under development.

Figure 9: The six main areas of applications.

Figure 9 illustrates the six main areas of applications that Teldat considers relevant for the branch office:

- **Security**. Applications offering security services for the communications: IDS, anti-virus, anti-spam, etc.
- **Telephony over IP**. Applications that offer ToIP features, such as local recording of ToIP calls or embedded IP PBX.
- **WAN optimization**. A set of applications that either improve the effective bandwidth available on the WAN or reduce the effective latency on the traffic, or both.
- **Management**. Applications that facilitate the work of the IT managers: Diagnose, SLA auditing, inventory, etc.
- **Green office**. Applications for a more efficient branch office: Digital Signage, office automation, etc.
- **Customer applications**. In this classification, all the applications developed by the customers themselves.

5.1. Security

Teldat has developed a security suite for its Atlas i60 enterprise branch office access router. The features of this security suite are well-known security functions on the market, that are available in many dedicated appliances (firewalls, UMTs, etc.), but some of them are also becoming part of the networking stacks of several established vendors, as yet another extra feature of their monolithic network operating systems. So, what is the deal with the Atlas i60? What are the advantages of the Teldat security suite applications on the Atlas i60? Or more properly, what are the advantages of running the security features as applications on the Atlas i60 instead of as features of the networking stack? There are two main advantages at least:

- **Performance**. In most, if not all, of those networking stacks that have security features, such as IDS, when you enable them, the throughput performance of the router drops drastically to a fraction of the performance of the same router with the

security features disabled. On the Atlas i60, since the security applications are run on a separate processor, the performance is much less compromised or even not changed, depending on the security application.

- **Flexibility**. Since the application execution environment on the Atlas i60 is standard and open, it is possible to integrate customer's own-developed security applications or even to integrate or license security technology from third parties on the market.

Improved security at the enterprise branch office is becoming a subject of great importance for several reasons:

- **Direct Internet access**. As described in section 2.2, the connection of enterprise branch office directly to the Internet is going to be an option, if not a need, motivated by the shift to the cloud computing paradigm and the available low-cost residential broadband services.
- **Internal hacking / security threats**. In a pure VPN branch office connectivity, the Internet related threats are handled centrally, at the single location where the connection to the Internet for all the VPN takes place. Nevertheless, this centralized topology does not control internal threats generated at the branch offices, such as own employees, Wireless LAN attackers at the branch, etc.
- **IPv6**. The new version of the Internet Protocol allows for a real end-to-end connectivity, where NAT is no longer a need for the Internet access. The IPv6 connected branch office is exposed to external attacks. This is a controversial subject and it does not necessarily mean a reduced level of security when using IPv6 as compared to IPv4, but it has to be managed.

Figure 10 shows a sample application to illustrate the growing importance of security at the branch office. Direct Internet access from the enterprise branch office is the best WAN optimization mechanism for the traditional enterprise VPN WAN, since it uses low cost broadband Internet connections to send bulk non critical traffic such as web or email, freeing the expensive VPN access for business mission-critical sensitive traffic. But this communications architecture requires advanced security features deployed directly on each remote branch office. These advanced security features can be implemented fully on the branch office access router or in a combination of this access router with a cloud-based Managed Security Service Provider (MSSP) service.

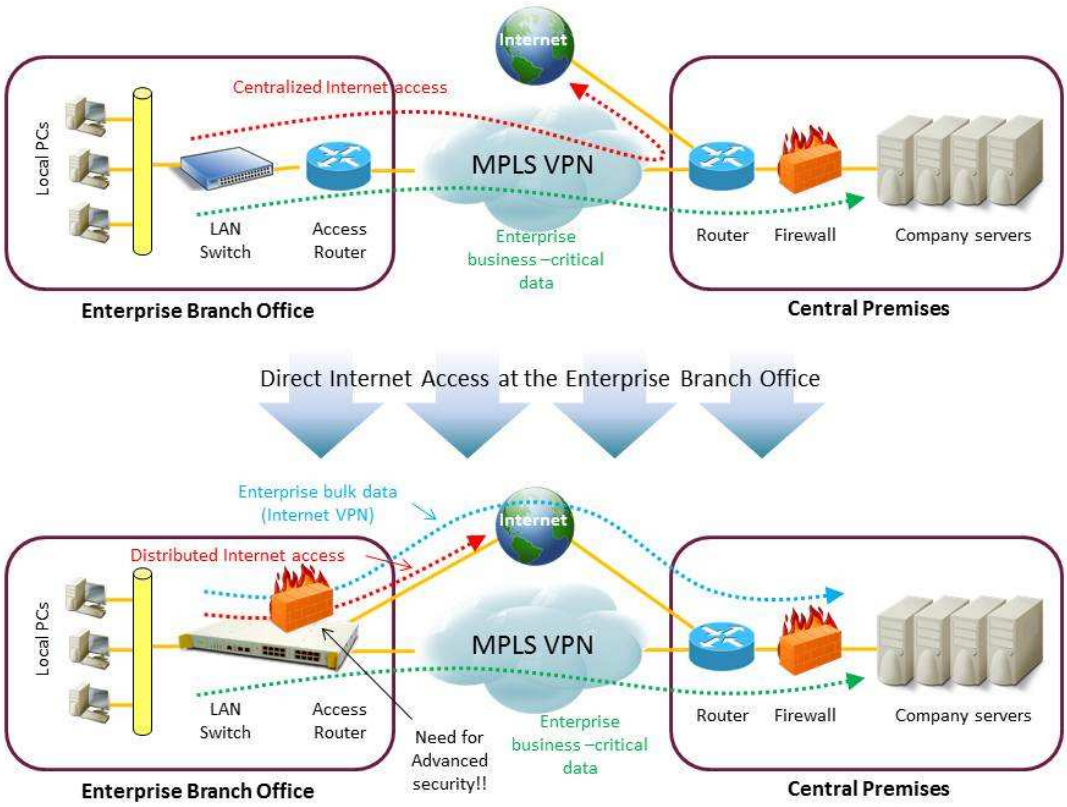

Figure 10: Direct Internet Access at the Enterprise Branch Office.

This is just a sample application to illustrate how security is a subject of increased importance in the new enterprise branch office access router. The following sections show the different applications of the Teldat security suite for Atlas i60.

5.1.1. Alien Vault certified OSSIM mini-sensor (IDS / Wireless IDS)

As every security deployment, a secured network has several levels of security and implements a range of security features or threat protections. One of such features is the "Security Information and Event Management" (SIEM), which analyzes the "thousands" of security events that the secure network generates to offer useful real-time security information to the security managers. The SIEM implements several key features within a secured network, such as data aggregation, alert system, dashboards and reporting or forensic analysis. But the most important security feature of the SIEM element is the correlation of security events, so that the huge amount of data coming from the events can be converted into useful information, reducing the occurrence of "false positives" and the number of undetected threats ("false negatives").Figure 11 illustrates the event correlation feature of a SIEM.

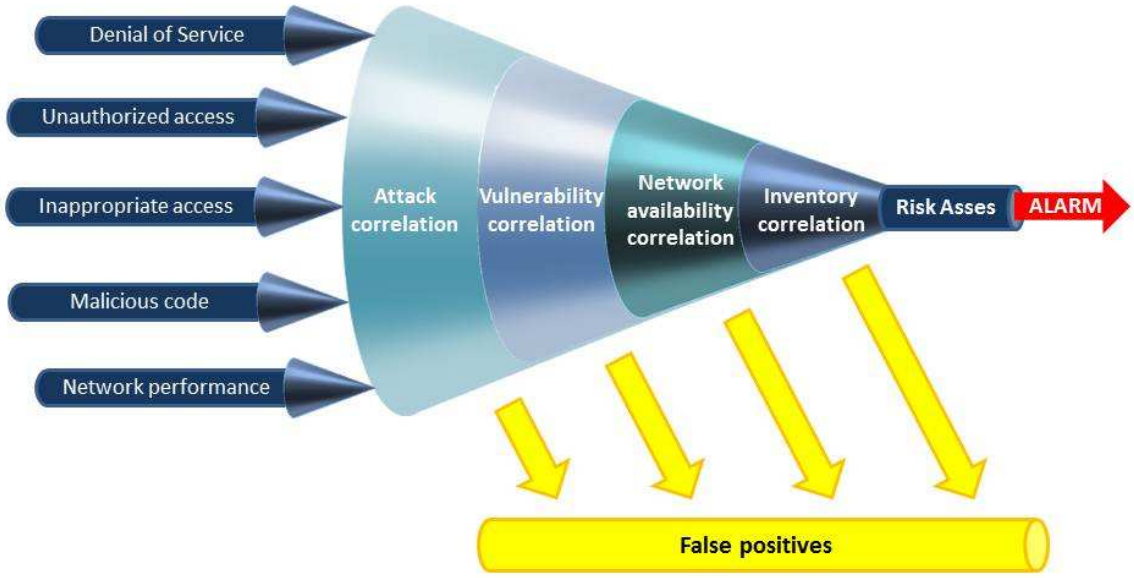

Figure 11: Event correlation feature of a SIEM.

This event correlation takes place in a central server or correlation engine, which receives security events from remote sensors or agents and, in general, from any network element with event reporting capabilities, such as servers, switches, routers, etc.

The main source of security events for a SIEM takes place under a security feature known as Intrusion Detection System (IDS). One remote IDS will analyze the traffic it sees against an extensive set of known attacks or threats (rules) and will send events when the inspected traffic matches one of the known threats.

One of the applications for the Atlas i60 cloud edge router that Teldat has developed is an Alien Vault certified OSSIM mini sensor[5]. The main feature of this OSSIM sensor is to act as an IDS and Wireless IDS (in case the Atlas i60 is equipped with embedded Wireless LAN connectivity) to detect threats and attacks on the remote branch office LAN and Wireless LAN infrastructure. This is a very interesting feature since, even in a VPN-only topology, central SIEM sensors will not be able to detect such remote threats: they do not see the traffic within the remote branch office LANs and a local dedicated SIEM sensor on that LANs is too expensive to make sense in most of the enterprise branch offices. Once again, the Atlas i60 applications positioning shown in Figure 4 is applicable for this IDS sensor application.

Figure 12 illustrates this IDS application on the Atlas i60 branch office access router. As can be seen on the figure, the Atlas i60 application allows for the protection of the branch office LAN and wireless LAN. The alternatives are (1) to use a dedicated SIEM sensor on each branch office, which is too expensive and so it rarely makes economic sense and (2) to enable IDS features on the "traditional" branch office router, which will plummet the performance and has also a much reduced set of IDS features.

Finally, Teldat Services Platform in the cloud allows for a convenient and integrated way to upgrade each remote Atlas i60 with the updated set of rules to detect attacks and threats. Another added value that Teldat offers is the smart selection of the rule sets, from thousands of available rules, to match threat analysis to the branch office configuration, minimizing the CPU load for a given branch office configuration.

[5] OSSIM is an open source Security Information and Event Management (SIEM). Alien Vault is the company that created OSSIM.

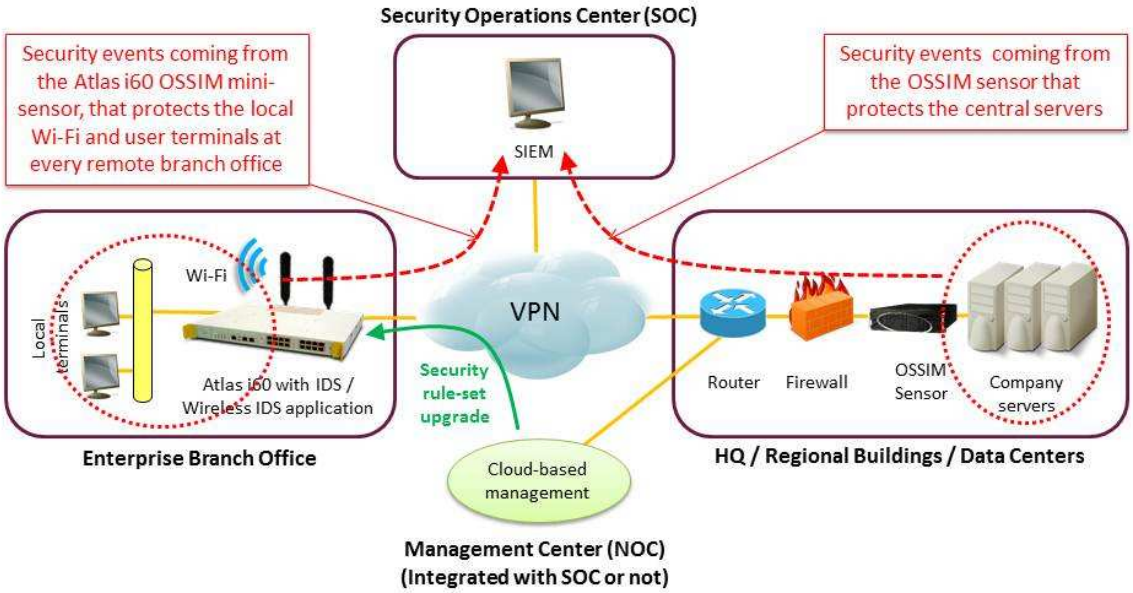

Figure 12: Alien Vault certified OSSIM mini-sensor (IDS / Wireless IDS) application on Atlas i60.

5.1.2. Secure web & e-mail suite

5.1.2.1 Anti-virus

The purpose of this application is to protect the branch office from Trojans, viruses, malware and other malicious threats coming from the Internet, the enterprise VPN or the local users at the branch office.

Why to implement an anti-virus application on the router? There are a several reasons:

- Cancel or at least isolate and block the infection at its originating location within the enterprise. The enterprise will surely have other anti-virus and security applications deployed at its central premises, especially to protect from external Internet attacks. But that central infrastructure neither necessarily secures or controls the threats generated locally at the branch office, nor prevents the infection from spreading within the VPN connected branch offices.
- This is especially important for direct Internet access at the branch office, as explained in Figure 10, since the branch office will be more exposed to external attacks.
- Better management in comparison with external dedicated security appliances.

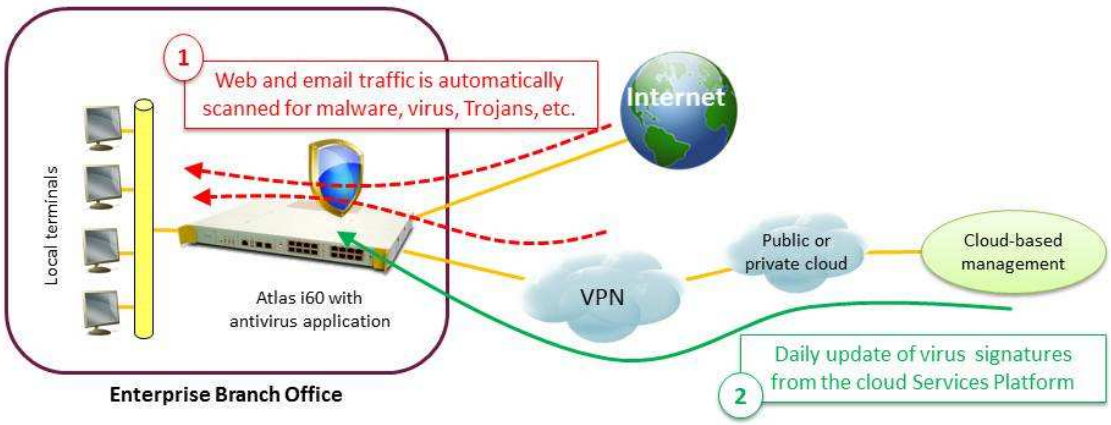

Figure 13: Anti-virus application on Atlas i60.

Figure 13 illustrates the Atlas i60 anti-virus application. A background process or application on the Atlas i60 runs transparently to the user and implements a web and email proxy.

This web and email transparent proxy intercepts such type of traffic and analyzes the files embedded (SMTP attachments, ActiveXs, etc.) as shown in Figure 14.

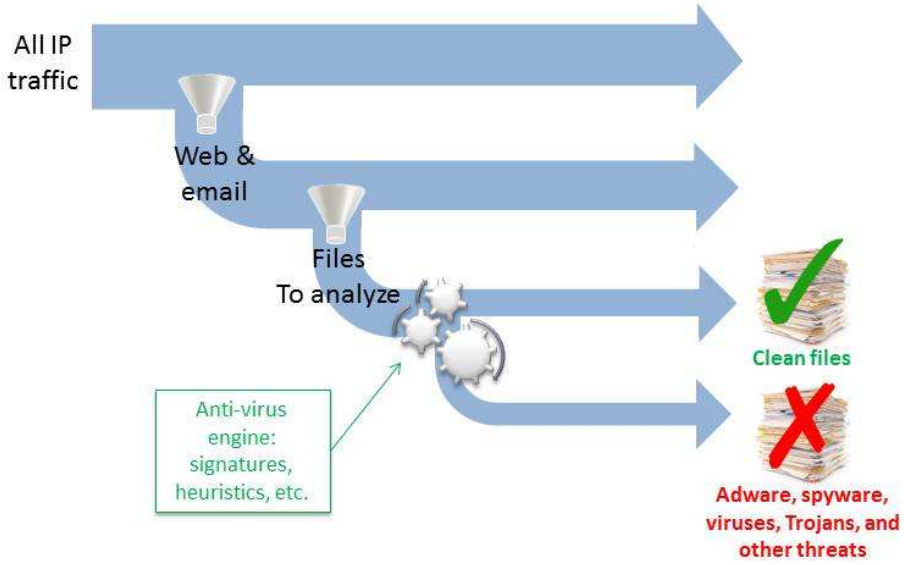

Figure 14: Anti-virus engine illustration.

The main features of the Atlas i60 anti-virus application are:

- Types of traffic analyzed: web and email.
- Supported email protocols: SMTP and POP3.
- Multiple compressed archive file types supported: Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS and others.
- Support for popular document formats including MS Office and MacOffice files, HTML, RTF and PDF.
- Daily incremental update of virus signatures from Teldat cloud-based Services Platform.

Teldat Atlas i60 anti-virus application is based on ClamAV well-known open source anti-virus toolkit. This example shows how the use of Linux on the second core of the Atlas i60 CPU allows for an easy integration of third party or open source programs for the benefit of the customers. Anti-virus is not an area of great expertise at Teldat, but by using ClamAV Teldat is able to integrate all its know-how into an integrated professional solution.

5.1.2.2 Anti-spam

The anti-spam application on Atlas i60 protects local branch office users against spam emails, i.e. unsolicited, undesired, or illegal email messages.

If normally a corporation will already have anti-spam protection on its central email servers, why to use an anti-spam application on the branch office access router? As in the anti-virus case, there are several reasons:

- To block the spam at its originating location within the enterprise. The enterprise will probably have an anti-spam application deployed at its central email server. But the Atlas i60 application blocks the outgoing spam before it even reaches the company email server and potentially spreads to other employees or contacts.

- The employee at the branch office could potentially access over the Internet to other external email servers, not controlled by the company. It is true that the company firewalling policies can filter out this traffic, but depending on the company's Internet access policy, it is not always the case.
- To add extra security or anti-spam protection. Even if the company has its own anti-spam application on the central email server (which is always true for big enterprises, but not so true for smaller ones) the use of the anti-spam application on the Atlas i60 introduces another source of protection and anti-spam policies.
- Better management in comparison with external dedicated security appliances.

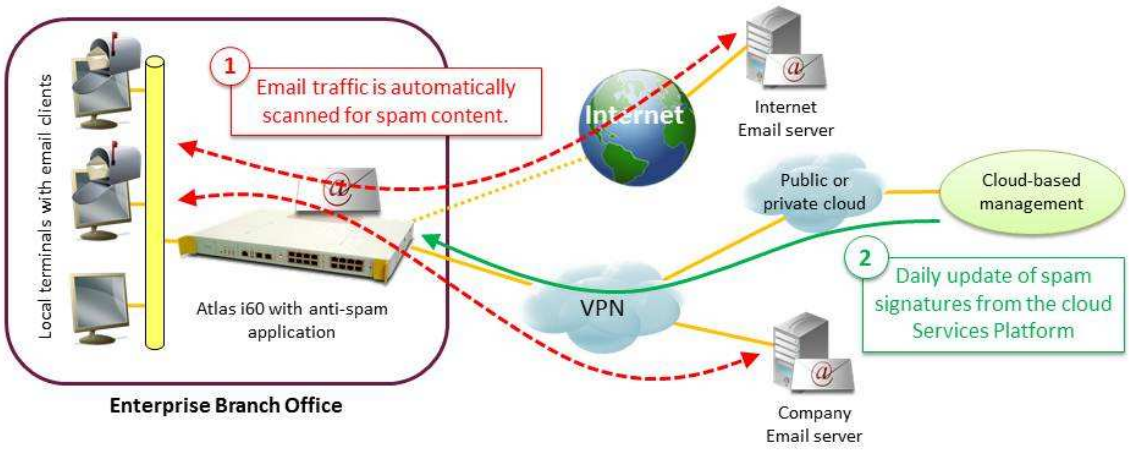

Figure 15: Anti-spam application on Atlas i60.

Figure 15 illustrates the Atlas i60 anti-spam application. A background process or application on the Atlas i60 runs transparently to the user and intercepts the email traffic, analyzing it for spam. Both incoming and outgoing email traffic is analyzed. A daily set of anti-spam rules can be updated from the cloud-based Services Platform.

Teldat Atlas i60 anti-spam application is based on SpamAssassin, a mature, widely-deployed open source project that serves as a mail filter to identify spam. It uses a variety of mechanisms including header and text analysis, Bayesian filtering, DNS blocklists, and collaborative filtering databases. As with the anti-virus applications, with the use of third party software, Teldat is able to integrate all its know-how into an integrated professional solution.

5.1.2.3 Content filtering/URL categorization/IP reputation

The Atlas i60 content filtering application protects the branch office against the access to malicious Internet servers. It also protect against servers whose content although, not malicious, is not allowed by the company policies.

When a VPN is used (normal case) an enterprise can control and limit the Internet access centrally, at the central firewall that controls the Internet connection. In this case and if the enterprise already has a content filtering application in place, the Atlas i60 application will not be needed. Nevertheless, there are some other situations in which local content filtering at the branch office is valued:

- When **direct Internet access** is used at the branch office, as explained in Figure 10, since the central control does not cover this direct access.
- When the use of **NAT at the central premises** on the Internet access avoids a detailed control on the Internet access. The application on the branch office can offer bigger control and detailed reports on the Internet use.

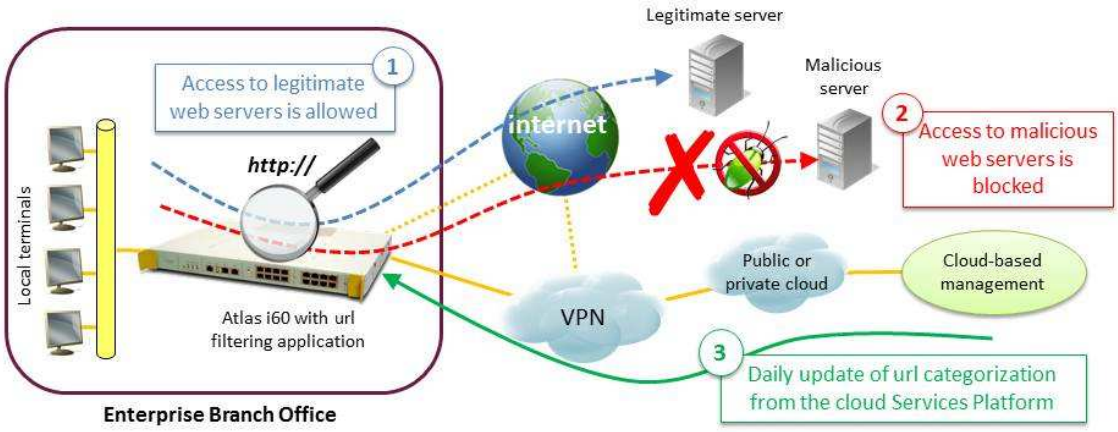

Figure 16: Content filtering, URL categorization and IP reputation application on Atlas i60.

Figure 16 illustrates the Content filtering, URL categorization and IP reputation application on Atlas i60. The application transparently intercepts the web access requests and checks them against url categorization databases. If the reported categorization is allowed, the web access request can go through and the access is granted. But if the categorization is disavowed, the access is denied. A given url can belong to several categories for a more grained control. IP reputation will control also the IP address of the given url and if the address reputation is not enough, the access will be denied, no matter what categorization the url has.

Like with the rest of the applications on the security suite, the cloud-based Services Platform allows for a unified and daily update of the url categorization databases.

Teldat Atlas i60 url categorization application is based on SquidGuard, a well-known open source project that allows for the use of third parties black lists and categorization databases.

5.2. WAN optimization

This category aggregates a group of applications that share the common goal of optimizing the WAN, improving the effective throughput or reducing the effective latency of the final user traffic on the WAN.

5.2.1. VideoProxy

VideoProxy is a live video splitting application. It allows multiple users on the LAN of a branch office to watch a live video stream without congesting the WAN, since the video stream is transmitted just once on the WAN, instead of multiple times.

Today, in a normal scenario, when multiple users on a branch office LAN want to watch a live video webcast, for instance “the president speech”, each one of them has to open a TCP connection to the central premises transmitting the webcast and so, the same video stream is transmitted multiple times in parallel in the WAN link, wasting precious WAN bandwidth and overloading the video server. As a consequence, almost no organization is really using live webcast on their branch offices today.

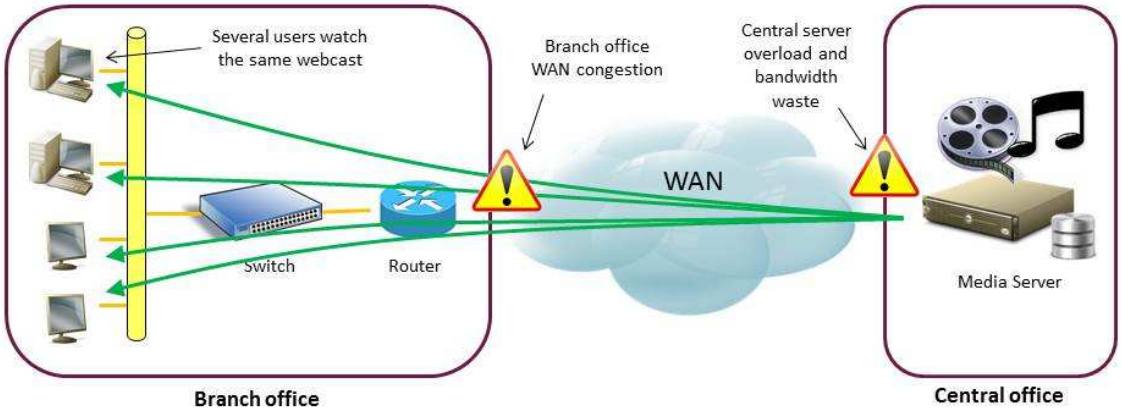

Figure 17: Challenges of enterprise live video distribution.

As Figure 17 shows, WAN bandwidth and server load are the most relevant problems when transmitting live webcast traffic to multiple remote users. Multicast is not an option either, since it is not used or supported in the most widely used video transport protocols, which use point-to-point TCP connections.

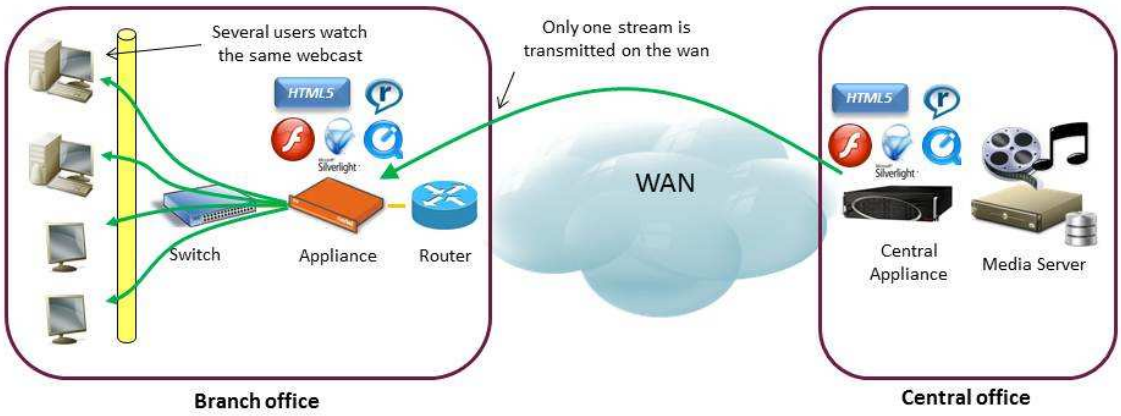

Figure 18: Video-splitting technique.

To solve this problematic, a technique called “video streaming splitting” transparently captures and terminates the video requests on the LAN and unifies them into a single request to the central site on the other side of the WAN. This usually requires the use of dedicated hardware at the branch office and normally also at the central premises, as Figure 18 shows. The appliance-based solution is very powerful (normally other WAN acceleration techniques will be available) but also very costly, both in CAPEX and OPEX, especially for small branch offices, where the customer might be force to pay for other features not really required (potential lock-in).

This is where Teldat solution, based on Atlas i60, enters the scene. As Figure 19 shows, instead of using external appliances, Teldat performs the video-splitting technique in the access router, particularly with an application that runs in the Linux core of the Atlas i60.

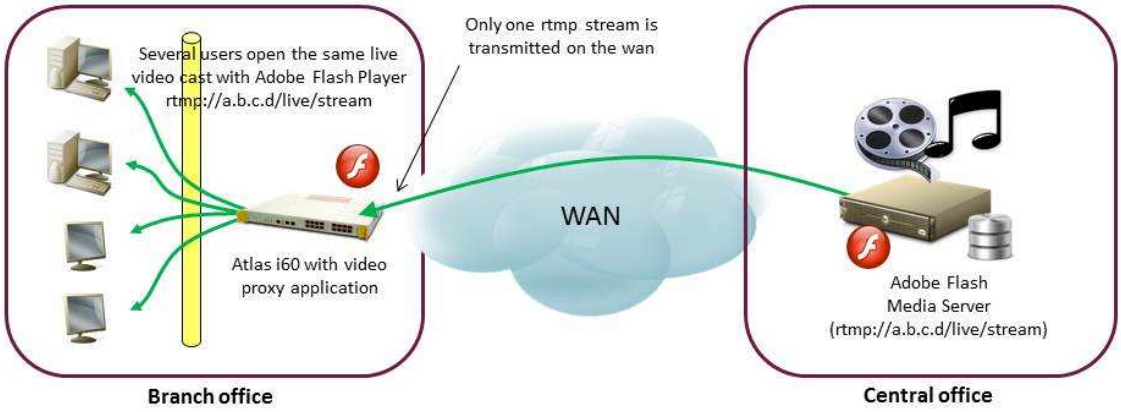

Figure 19: Teldat solution for video splitting.

Teldat solution has a series of advantages over existing market solutions:

- No extra hardware is required in the central and remote locations: lower CAPEX.
- Integrated management and single box solution: lower OPEX.
- Transparent to the user: no changes / agents required on the video player.
- Modular solution: deployed Atlas i60 devices can be upgraded to support the VideoProxy application: reduced initial investment.
- The branch office switch might also be removed, since the Atlas i60 embeds a 8/16 ports switch.
- Compatible with central WAN acceleration appliances and CDNs that the corporation might have in place for bigger regional offices or central services.

Today, the VideoProxy application supports Adobe Flash video transport protocol, but it is been extended to support other protocols such as Silverlight from Microsoft and HTML5.

5.2.2. Web cache

Web cache is a very useful functionality for many enterprise branch offices.

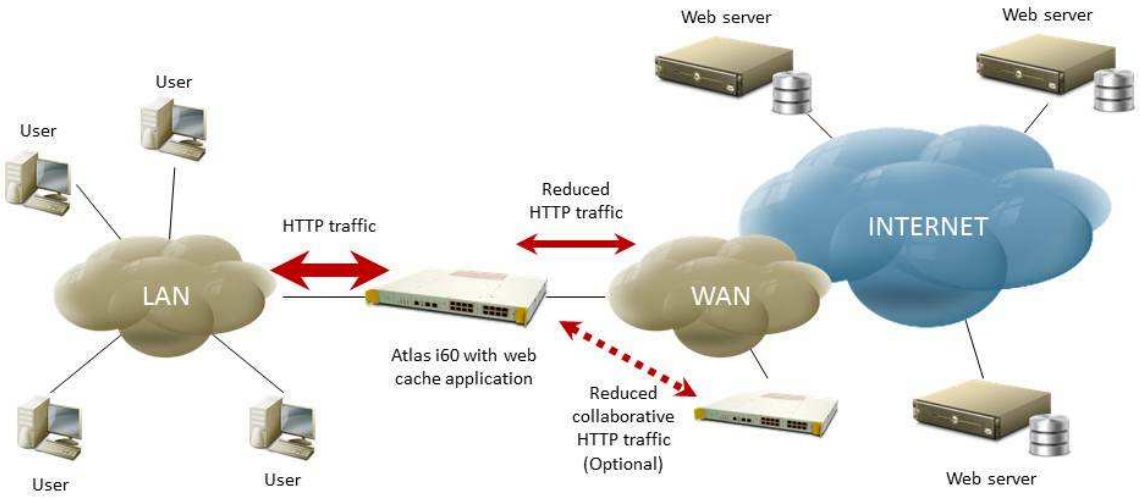

Figure 20: Web cache application on Atlas i60.

This well-known feature, illustrated in Figure 20, intercepts the Internet traffic that the users on the enterprise branch office LAN are downloading and stores a copy locally, so that the next user requesting the same information will received it from the locally stored copy, instead of downloading it from the Internet again. This is a WAN optimization technique that saves bandwidth; the more users access the same information, the more bandwidth it saves.

For this reason, this application will be useful for branch offices in which their local users access frequently a common set of information that is able to be cached. For instance, education is a very interesting market, since the students will normally download the same information on a given course: the course materials.

By using the Atlas i60 web cache application, corporations can save the investment on external dedicated web cache appliances at the branch offices. An external appliance will have more performance (more storage space and more aggregated bandwidth serving capabilities) but will be more expensive and will not be economically justified, especially on small branch offices.

5.2.3. Cloud-synchronized NAS

Another technique, very interlaced with the cloud computing architecture is the use of local storage at the branch office, but synchronized under certain policies with a centralized cloud-based storage infrastructure.

For small enterprises, just the simple use of a Network Attached Storage (NAS), periodically backed up offsite, will probably do. For this market, the Atlas i60 has also a "simple" NAS application that allows the internal hard disk to be shared on the LAN, with capabilities to configure users, permissions and disk quotes to be used, and the possibility of periodic or manual backup in the Services Platform cloud.

But bigger or more demanding companies require more advanced features, both on the NAS customization possibilities and on the requirements of the cloud service to be used. Figure 21 illustrates this scenario.

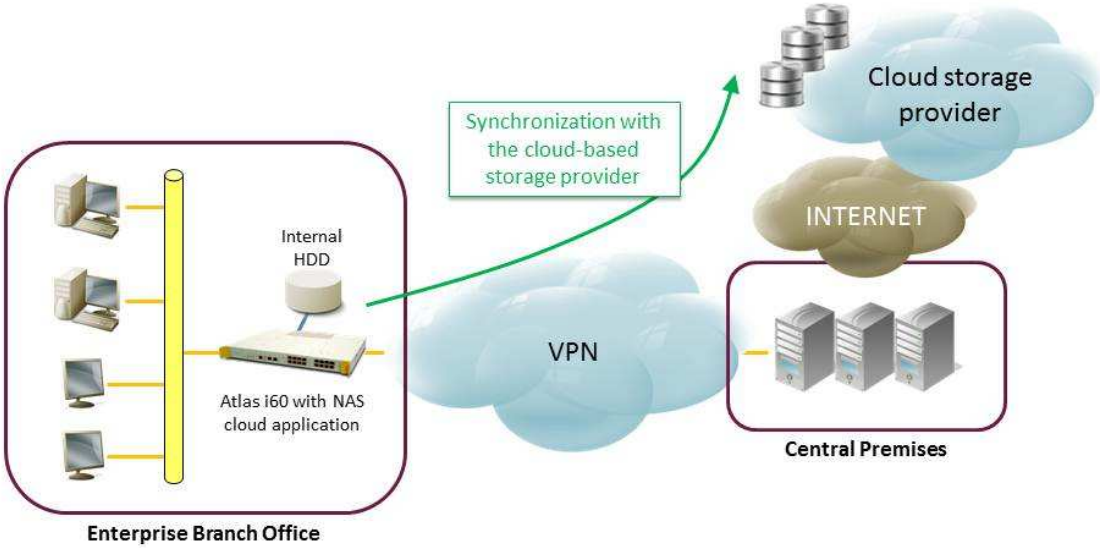

Figure 21: Atlas i60 cloud-synchronized NAS.

These advanced features are related mainly to three areas:

- **Performance**. A transparent LAN speed access to storage services is required. This is trivial for standard NAS, but not so easy for cloud-based storage. So, an application that transparently provides this wire-speed cloud storage functionality makes all the sense. This wire-speed performance is achieved with advanced techniques as de-

duplication and smart cloud synchronization, in which the user PC works with the local storage, which is efficiently synchronized with the cloud storage provider in parallel.

- **Security**. Relying on a third party storage provider requires security because the organization's critical data is going to be in someone else's hands. So, the cloud storage has to encrypted and a secure architecture in place.
- **Integration**. Flexibility to access the data on the cloud is also a key need of corporations, which eventually will need that information from different business applications. So, standard-based mechanisms for data access will be needed, both on the LAN side so that the branch office applications do not need to change (for instance, no proprietary agent or software on the local PCs), but more importantly on the cloud side, so that the data is accessible from any enterprise application that requires it.

5.3. Telephony over IP

5.3.1. Local recording of ToIP calls

In some markets, like insurance or banking, some business processes involve the recording of voice calls[6]. Tier-1 voice solutions support this feature; usually in a centralized manner and oriented to some vertical markets like call centers, IVRs, etc. But call recording on the enterprise branch office is not properly solved in these centralized solutions:

- Internal calls (within the same branch office) are not supported.
- It is too expensive or inconvenient to implement, since all voice calls should be routed to the central point, which is too expensive to dimension, hard to provision and adds unnecessary delays to the voice calls.

The alternative to centralized call recording is local recording at the branch office itself. But this has its own inconveniences:

- A dedicated appliance / server is needed.
- The local LAN switch has to be configured in port-mirroring, if internal calls are to be recorded. This can be problematic and it wastes bandwidth.

[6] Since ToIP is steadily being adopted on the enterprise, this section will consider only ToIP scenarios.

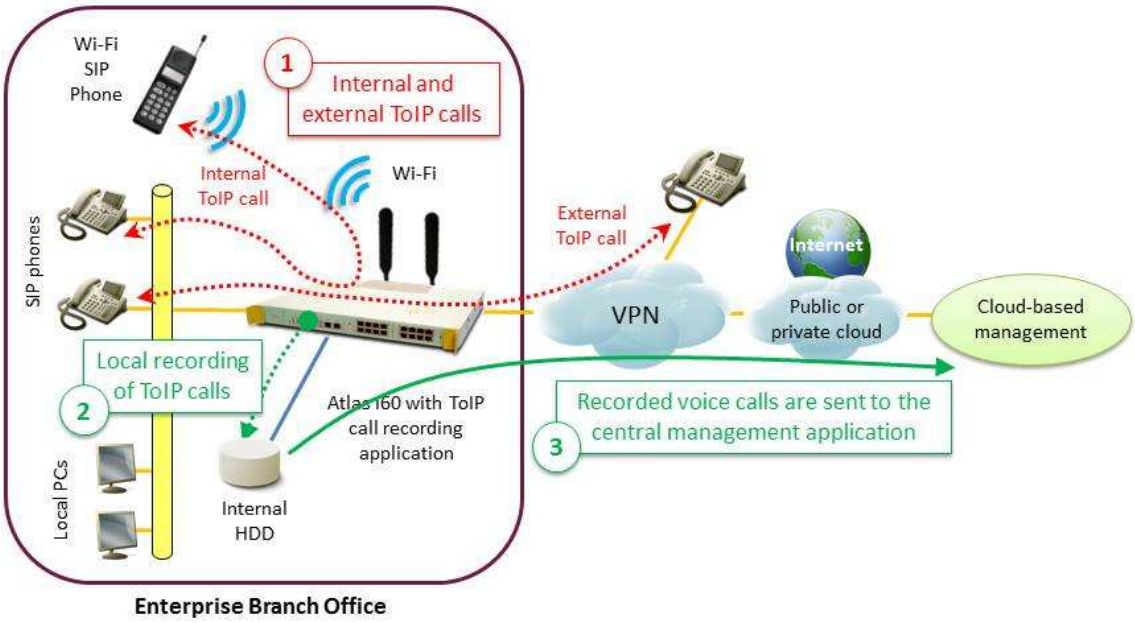

Figure 22: Local recording of ToIP calls.

As an alternative to the use of a dedicated appliance, Teldat has developed an Atlas i60 application for the local recording of voice calls, as described in Figure 22, whose main features are:

- Supported signaling protocols: not encrypted SIP and H.323.
- Supports internal (both peers on the same office) and external (one remote peer) calls.
- Supports incoming (externally generated) and outgoing (locally generated) voice calls.
- Supports wired LAN and wireless LAN ToIP phones.
- Selective or on-demand recording.
- Recorded voice calls are locally stored in the internal hard disk to be sent to the central systems when configured, for example during night time, when the pipe is less used.
- Classification and tagging of recorded calls: time-stamping, duration, involved parties, codec, etc.
- Optional encrypted storage of the voice calls on the internal hard disk.
- Independent of the ToIP solution deployed at the branch office: The Atlas i60 does not have to be an element of the ToIP solution, such as the media gateway or the local IP PBX (although of course it could be).

Finally, for a better performance, a smart port-mirroring auto-configuration feature of the Atlas i60 embedded switch reduces the LAN bandwidth consumption and the load of the CPU. Nevertheless, the use of specific VLANs or the connection to predefined physical ports of the switch for the ToIP phones it is recommended, although not mandatory.

5.4. Management

This section describes applications that facilitate the work of the IT managers themselves: Diagnose, SLA auditing, inventory, etc.

5.4.1. Inventory

As shown in Figure 23, the Atlas i60 Inventory application discovers and classifies the networked devices found in the branch office. It also consolidates this information database in the cloud.

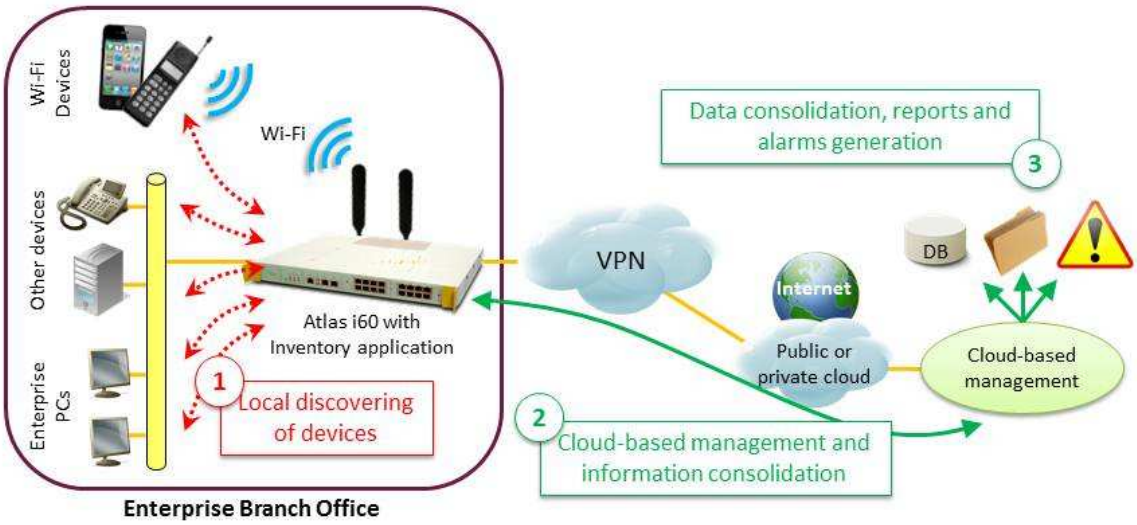

Figure 23: Atlas i60 Inventory application.

Enterprises might already have an Inventory application in place, using dedicated appliances and software, but as with the rest of the Atlas i60 applications, the use of the Atlas i60 for this task will be much more cost-effective.

The main features of the Atlas i60 Inventory application are:

- Active / passive discovering modes. Active mode (injecting dedicated traffic on the network) will be faster and will be able to discover more parameters, but it will load the Atlas i60 Linux CPU more than the passive mode (discovering devices and some of their properties by just listening to the traffic on the network).
- Automatic (background always-on process) or manual operation.
- Support for local wired and wireless LAN interfaces on the Atlas i60.
- Rich inventory: the amount of information that can be discovered depends on the discovering mode (active/passive) and on the configuration/features of the discovered machines, but a sample of the parameters that can be discovered is:
    - Hardware information (type of machine, CPU, etc.),
    - Operating system used and other information from the OS.
    - Operation intervals of the machine.

5.4.2. NTOP: Traffic visualization / characterization

Teldat has integrated NTOP into the Atlas i60 application server. NTOP is a well-known open source network traffic probe to see the network usage. The main feature it supports is Deep Packet Inspection (DPI): application-layer detection of protocols, independent of the port the application is using. For instance, it is possible to detect Skype over http.

In many organizations IT managers have a difficult time to diagnose network problems that occur on their remote branch offices. The tools available on standard networking gear are not enough in many situations and often IT managers have to deploy a dedicated network probe at the branch office, or at least they wish they could.

Embedding that functionality on the Atlas i60 offers a very convenient price/performance trade-off. The dedicated appliance will be very powerful (meaning for instance it will be able to analyze higher throughput) but also very expensive, while the Atlas i60 NTOP application will not be so powerful but will have no match on cost. Besides, thanks to the internal Atlas i60

architecture, as explained in Annex 2, the normal communications performance of the router side will not be affected. This is especially relevant in this case, because the Atlas i60 could be routing normal traffic at 100 Mbps and at the same time performing DPI on the traffic at 50 Mbps: some traffic will be lost for the analysis, but not for the communications.

Another advantage for the IT managers is that they will be able to analyze the LAN traffic, that is not necessarily routed to the WAN and so it would not be seen on the central premises even if a probe would be placed in that central location.

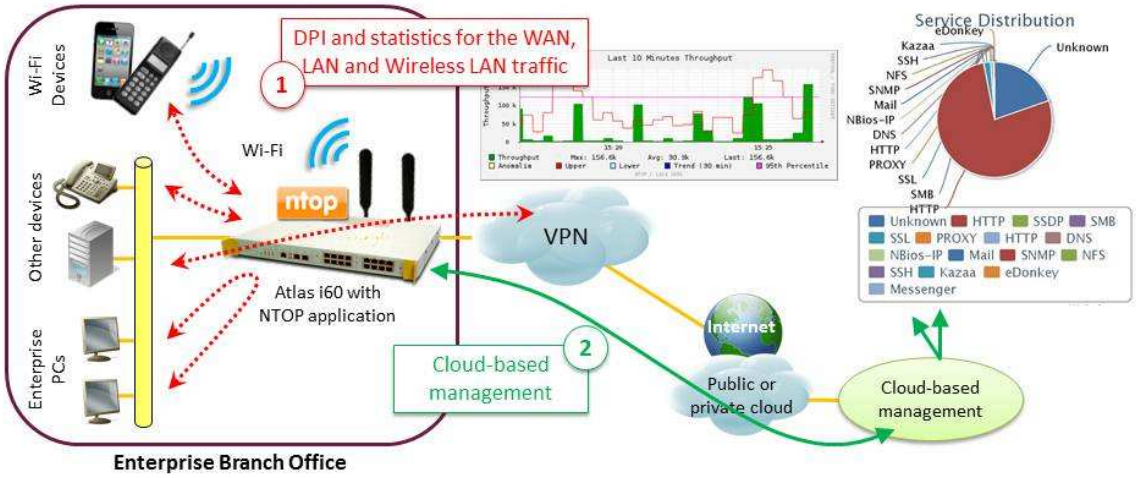

Figure 24: NTOP application on Atlas i60.

Besides de DPI analysis, the NTOP application generates a lot of other statistics:

- Sort network traffic according to many protocols.
- Display traffic statistics.
- Show IP traffic distribution among the various protocols.
- Analyze IP traffic and sort it according to the source/destination.
- Display IP Traffic Subnet matrix (who's talking to who?).
- Report IP protocol usage sorted by protocol type.
- Geographical map of hosts.
- And many others.

5.5. Green office

5.5.1. Digital Signage

Digital signage solutions allow for the dynamic display of marketing and sales information on public displays, in places such as financial entities branch offices, kiosks, transportation networks, hospitals, etc.

Today's solutions are very powerful and customizable, but at the expense of a high cost of acquisition, installation and operation. They feature a great deal of options on the multimedia content that they are able to prepare and display. But the reality is that existing solutions are too expensive for the medium/small branch office.

Teldat proposes a low-cost Digital Signage solution, with a reduced set of features compared to a dedicated Digital Signage solution, but with enough features for most of the customer scenarios.

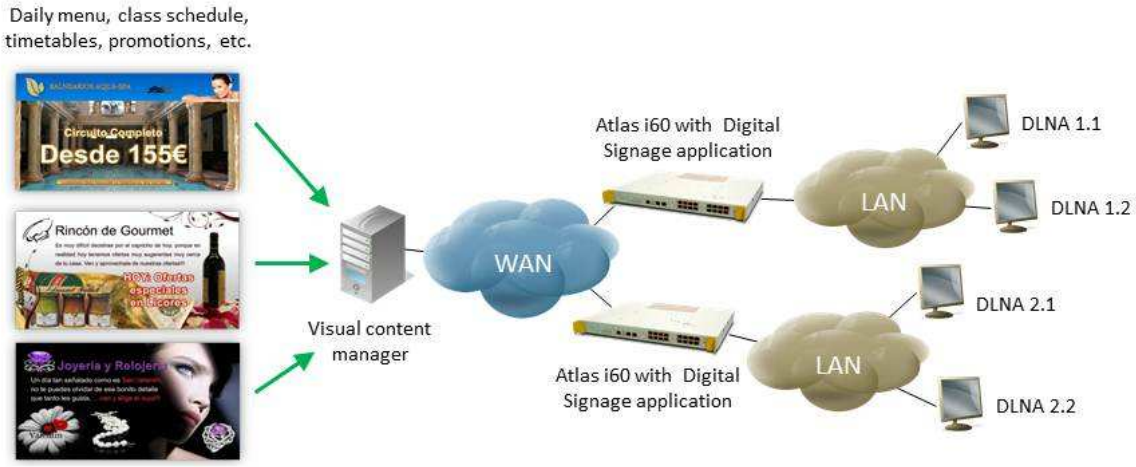

Figure 25: Atlas i60 Digital Signage scheme.

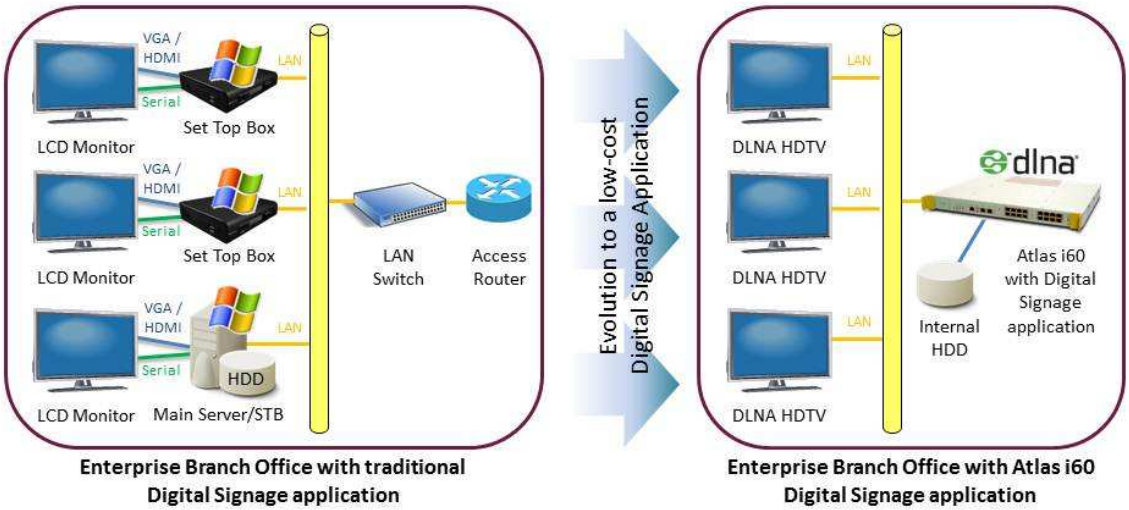

Figure 26: Evolution to a low-cost Digital Signage Application.

Figure 25 depicts the overall system while Figure 26 highlights the technical elements that permit a considerable cost reduction. As shown, the cost savings due to the use of the Atlas i60 Digital Signage application are coming from:

- **Professional LCD monitors** are replaced by consumer DLNA TVs.
- **Set-Top-Boxes** are replaced by the Atlas i60 application that embeds a DLNA media server.
- **Windows licenses** of the STBs are no longer needed.
- The **LAN switch** can be replaced by the Atlas i60 embedded switch.
- The expensive and difficult-to-install **video cables** (VGA or HDMI) and **serial cables** are replaced by affordable and probably already existing Ethernet STP structured cabling.
- The **central Digital Signage server**, used for content preparation and schedule, is replaced by Teldat's cloud-based Services Platform (SaaS).

But what is the trade-off? The limitations of Teldat solution are:

- Just a single multimedia content can be sent to a single TV, although different TVs can play different contents at a given time. This limitation comes from the use of DLNA,

which allows for the elimination of the STBs (because the content render or player is now the TV itself) but permits only one single multimedia flow (images, audio or video) to be played at the TV. DLNA restricts also the multimedia codecs and containers that can be used, although the supported ones are enough for most needs.

- Power ON/OFF. The DLNA standard does not foresees the TV power on or off command, so this feature is either not supported or it has to be supported with Wake-on-LAN commands and proprietary shutdown commands.
- Simple easy to use central Visual Content Manager Server, probably not as featured as other commercial solutions, although good enough for many customer scenarios.
- Limitations coming from the Atlas i60 performance: limited storage space and memory, number of HD streams supported, etc.

5.6. Customer applications

This category groups all the applications developed by the customers themselves.

This section simply highlights the fact that Teldat offers an open system, in which the customer does not depend on the applications developed by Teldat but can develop its own applications.

As Figure 27 illustrates, this open environment is offer through the use of a standard Linux kernel (2.6.31 version), the full Debian distribution including its packing system and the support for a Java Virtual Machine.

Figure 27: Environment for the development of user applications.

The development environment consists of a dedicated Atlas i60 router with all the development tools ("*toolchain*") available for the customer, which has also access to a full Debian repository and can develop applications in a wide range of languages, such as C/C++ or Java.

Annex 1: Features of the Atlas i60 as an Enterprise Branch Office Access Router

Interfaces and modularity

The Atlas i60 supports the following list of interfaces and expansion slots:

- 2 x 10/100/1000 WAN Ethernet ports, RJ-45 connectors
- 8 x 10/100 LAN Ethernet ports, RJ-45 connectors, with optional PoE
- 1 x Expansion slot for 8 extra LAN ports. Available cards: 8 FE ports and 4 GE ports
- 1 x USB 2.0 host port
- 1 x Expansion slot for xDSL cards
- 1 x Expansion slot for generic voice/data interface cards compatible with all Atlas routers (PMC standard form factor). Available cards: E1, ADSL2, G.SHDSL, VDSL2, 2xGbE SFP, 3xSerial, 4xSwitch, PSTN analog modem and a range of ToIP media-gateway cards: PRI, BRI, FXS, FXO, E&M
- 1 x Wireless-WAN expansion slot, for embedded 3G/4G modules with external detachable antennas, SMA connectors
- 1 x Wireless-LAN 802.11 a/b/g/n expansion slot with external detachable antennas, SMA connectors
- 1 x Expansion slot for storage (SATA hard disk / solid state drive)
- 1 x Console port, RJ-45 connector

Hardware architecture

Processor: P1020E Freescale - Core 2xE500v2

- 800 MHz
- Hardware encryption

Memory

- Flash 64 MB
- Total RAM 512MB (CIT uses 128MB and Linux uses 384MB)

Storage

- USB: 4Gb. Speed 10Mb/s – 1,25 MB/s
- HDD: 250GB. Speed 480Mb/s – 60 MB/s
- RAID --- No

Networking stack

All Teldat routers for the enterprise run the CIT software stack, a proprietary, full-featured professional grade networking stack. Figure 28 summarizes its main high-level features. For a more detailed list of the software features supported, please check the Atlas i60 datasheet at www.teldat.com

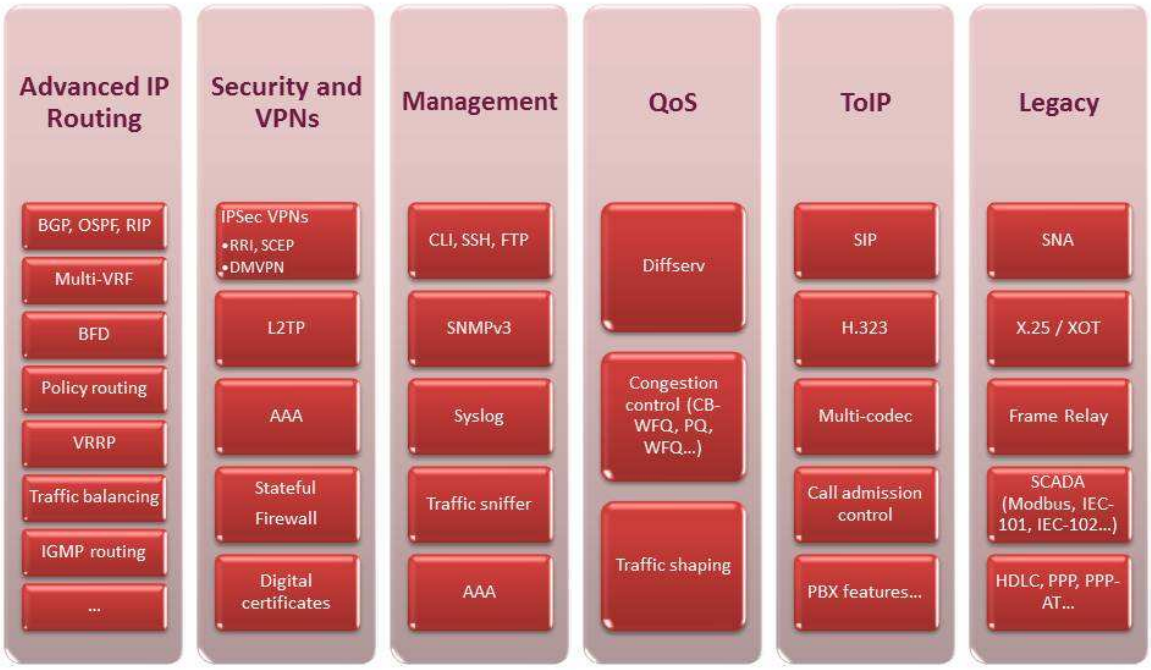

Figure 28: Professional networking software stack.

Performance comparison

As an enterprise branch office access router, the Atlas i60 achieves one of the highest routing performances on the market, as can be seen in Figure 29.

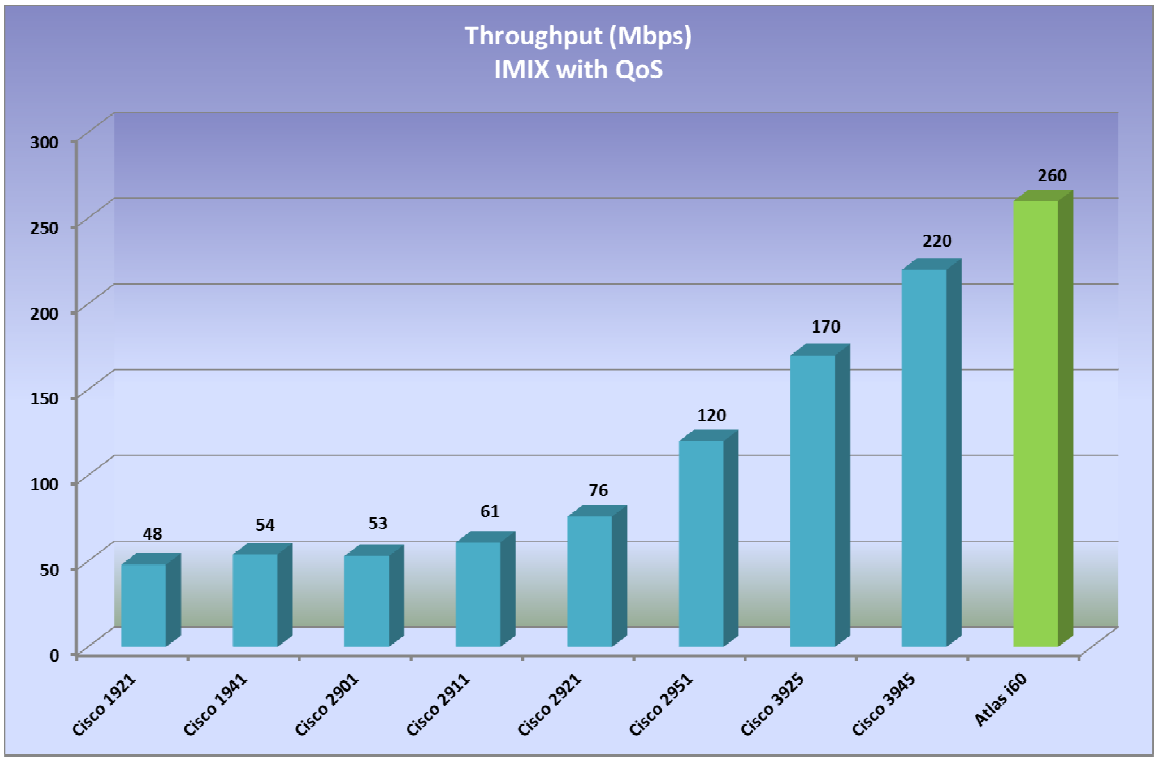

Figure 29: Atlas i60 - Cisco Throughput comparison chart. IMIX traffic with QoS. Bidirectional: value is per direction.

This comparison chart has been elaborated by a Tier-1 carrier, as part of the certification process of the Atlas i60 router into its Metro Ethernet managed service for corporations. So, the chart reflects a fair comparison since (1) all the routers are tested in the same scenario and (2) the tests themselves have been made by an independent part. Besides, the test scenario is a realistic complex one, not the best case scenario; it includes access lists, QoS, IMIX traffic (small packets), routing features, etc. The chart shows how the Atlas i60 is way more powerful than well-known Cisco routers. For instance, the throughput that the Cisco 2911 branch office access router can achieve is only 24% of the Atlas i60 in the same conditions!

Similarly, Figure 30 shows the throughput comparison chart for IPSec traffic, where the Atlas i60 advantages over Cisco are pretty much the same than for non-encrypted traffic.

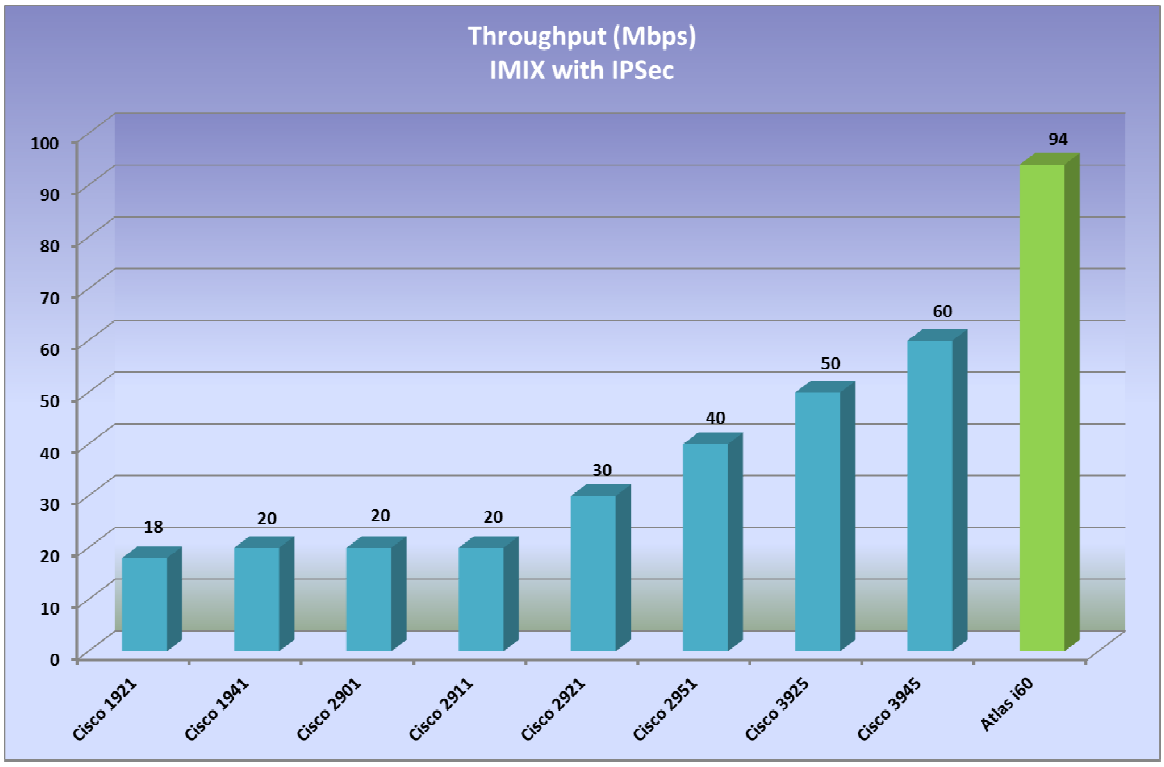

Figure 30: Atlas i60 - Cisco Throughput comparison chart. IMIX traffic with IPSec. Bidirectional: value is per direction.

Annex 2: Atlas i60 internal architecture

This annex outlines the Atlas i60 internal architecture, as background information for a better understanding of the other sections of the whitepaper.

The Atlas i60 is powered by a dual-core CPU. The core reserved for the applications runs on Linux operating system, with kernel version 2.6.32 and a Debian-based distribution. It also supports JAVA 6.

Peripheral & memory sharing

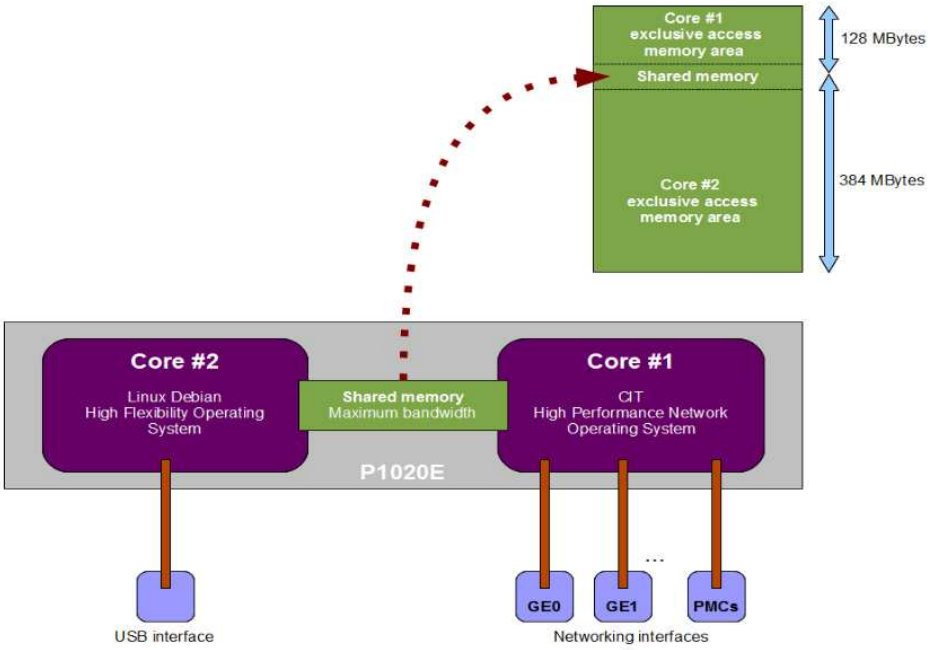

Figure 31: Peripheral and memory sharing on Atlas i60.

Figure 31 shows how the two cores share the physical memory and networking interfaces. From the peripherals point of view, the Core #2 (Linux) handles only the only USB physical interface. All other are handled by the other core.

The 512 Mbytes of memory are logically divided between the two cores. The first 128 Mbytes have been assigned to the Core #1 and the 384 Mbytes remaining to the Core #2 (Linux).

Communication between cores is done by means of a shared memory area mapped on the MMU of both cores. Over this area a MPI (Message Passing Interface) has been implemented and a “Shared Ring Buffer” is used for packet passing between cores.

This architecture allows for a maximum bandwidth throughput between cores.

Today, only layer 3 (IP) interface is supported between the two cores. It means that the Linux core is able to receive only IP packets from the CIT, although layer 2 (Ethernet) interconnection is under development.

Basic networking (server only)

From the CIT point of view the “Application Server” is like a host with an IP address that is configured in the CLI inside the “feature vli” menu.

As shown in Figure 32, all the packets received by the CIT destined to this “local” address are sent to the Linux.

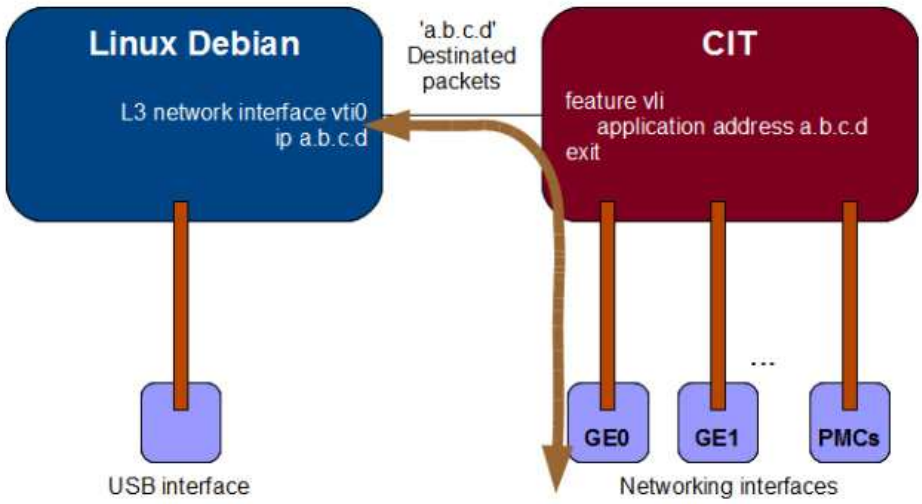

Figure 32: "Host" type interconnection between CIT and Linux.

Advanced networking

Fig xx shows a more advanced networking scenario. An “access list” can be configured in such a way that all traffic matching this access list can be “exported” or “diverted” by the CIT to the Linux core.

“Exported” means that CIT is going to make a copy of the matching packet. The copy will be issued to the Linux and the original packet will be processed by the CIT forwarder as usual.

“Diverted” means that CIT is going to send this packet to the Linux without copying it. Then the packet will arrive at the Linux kernel and the CIT will no perform any extra processing on that packet, i.e. the packet will not be forwarded by CIT.

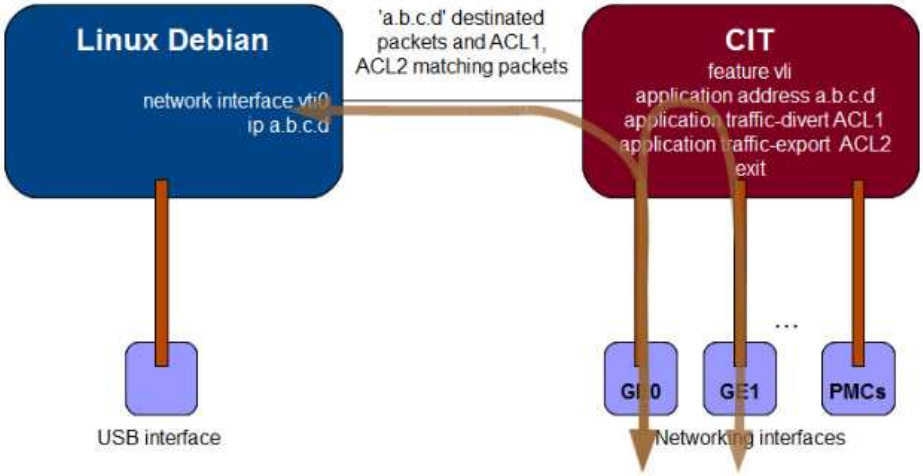

Figure 33: Advanced networking interconnection between CIT and Linux.

TELDAT DOCUMENTATION

This whitepaper shall be used only for information purposes. Teldat reserves the right to modify any specification without prior notice.

All trademarks mentioned in this document are the property of their respective owners. Teldat accepts no responsibility for the accuracy of the information from third parties contained on this document.

TELDAT S. A.
Parque Tecnológico de Madrid.
28760 Tres Cantos, Madrid
Spain
Tel.: + 34 91 807 65 65

Anna Piferrer 1-3.
08023 Barcelona
Spain
Tel.: + 34 93 253 02 22

TELDAT GmbH
Suedwestpark 94
90449 Nuremberg
Germany
Tel.: +49 911 9673 0

TELDAT Mexico
Diagonal 27. Colonia del Valle
Mexico D. F. 03100
Mexico
Tel: +52(55)55232213

TELDAT USA
1901 S. Bascom Avenue, Suite 520.
Campbell
CA 95008
USA
Tel.: +1 408 892 9363

TELDAT CHINA
A 060, F10 SOHO Nexus Centre
No19A, East 3rd Ring North Road,
Chaoyang District
Beijing 100020
China
Tel.: +86 10 57351071