# A PERFORMANT ARCHITECTURE FOR DELIVERING INTERNET HIGH AVAILABILITY SERVICES

R. GRIGORESCU[1]

*Lucrarea se doreşte o analiză de caz bazată pe necesitatea construirii unei infrastructuri de acces Internet care să răspundă unor nivele ridicate de disponibilitate cât şi de utilizare eficientă a lărgimii de bandă. Sunt prezentate soluţii originale ce vin în completarea infrastructurii de injecţie Internet către utilizatori (reţea locală). Arhitectura este completată cu o soluţie de acces de la distanţă a resurselor utilizator din cadrul reţelei de date interne, prin intermediul mai multor medii de transmisie şi beneficiind de aceeaşi metodă de autentificare a utilizatorilor.*

*The paper is meant to be a case study based on high level of Internet access infrastructure availability and efficient bandwidth usage. There are presented original solutions that are overlapping with the user Internet traffic injection architecture. The platform is completed by a remote access solution over different media types and using the same method of user authentication.*

**Keywords**: Internet, VPN, firewalls, IDS, router, network traffic, authentication, bandwidth, token, BGP, routing-protocol.

## 1. Introduction

The Internet is a miracle of the modern world. We became very familiar in our discussions when we open this subject. Unfortunately, this endless network wasn't designed by anybody and is not being governed by too many rules. On the other hand, the advantages offered are far too many related with the existing limitations. There is no information that you are looking for, and not being mentioned something about-it on the Internet. Personally I consider that the Human kind lost something with this occasion (you can see fewer people in museums, art galleries, opera, etc.); or,... maybe I'm wrong.

Because of the extreme openness of the Internet and in order to provide this kind of related services to financial institutions, you have to be prepared to take a lot of precautions. Not everybody in this world is using the Internet access in a "positive", or at least "not destructive" way. Probably you will be surprised if I tell you that based on my traffic analysis and log calculations, there are peak

[1] Ph.D Student, University POLITEHNICA of Bucharest, Romania

periods, when “The America is awakening”, as I like to say, when can be recorded even 300 simultaneous “attacks” from the Internet. These attacks, represents ways of trying to gain control of different network equipments, to affect their performance, to scan for different services available in order to disrupt them, etc. There is something amazing in this fight ”Attackers versus Defenders”; 90 % of the recorded attacks are just for fun...

In order to avoid these dangerous situations, is mandatory required to use special devices (firewalls) [1]. These equipments are performing based on some very simple principles:

- Any request of a new connection establishment, service activation, query, etc., came from the outside world (Internet), is rejected by default, not providing any feed-back to the initiator. The default behavior can be changed by special statement carefully monitored afterwards.
- Any request of new connection came from the inside area (trusted zone) to the outside (not-trusted Internet), is permitted, but with a lot of supervisory tasks from the firewall side. This device monitors all the established connection and if there are recorded long periods of inactivity or weird packets that are not conforming to the expected sequencing, the connections is dropped.
- The demilitarized areas (DMZ), have a special statute. Are logically positioned between the trusted area (inside) and the not-trusted one (Internet). This DMZ’s can have both trusted role and not-trusted role, depending where the traffic is initiated from. If the “inside” area is initiating connections to the DMZ, these connections are allowed by default, with the supervisory rules mentioned above. If the “outside” area is initiating connections to the DMZ, these are banned by default. Of course, all these default behaviors can be changed by the security administrators, but with much care and monitoring activities afterwards.

If we consider that the most part of the user protection is automatically accomplished by the firewalls, is important to mention that, these devices can be by themselves the prime target of the Internet attacks. In this respect, is very important the initial and the later on security policies applied, these equipments should be as “stealth” is possible to the outside world. Another problem is related with the router placed in front of the firewalls, which actually makes the Internet connectivity. Being a network device, it should be carefully configured by not letting any service opened to the outside world. The “stealth” policies should be

applied also, the service availability being dependent also by this equipment. There are brands specialized in building routers, that can actual integrate inside the operating system, some firewall features that can provide extra-protection.

## 2. The principles of the proposed Internet access architecture

The Internet access architecture I built, was designed in order to preserve as much is possible the available Internet bandwidth, in order to keep a low level for the running costs, being able in the same time to guarantee minimum bandwidth requirements for some groups of users and all of it with a high level of service availability.

Usually, inside the Internet providers market, everybody is talking about the last mile (user access) bandwidth. Usually, the ISP's (Internet Service Providers) are paid for the limited bandwidth that comes to the users door and sometimes even for the total amount of traffic made by the user on the Internet access provided.

For the Romanian Internet market, there is a small trick...The Internet traffic can be differentiated in two categories:

- National Internet sites access (referred as "Metropolitan", or sometimes "RoNIX" [2]) and International Internet sites from all over the world. The difference between these two kinds of Internet traffic is very high related with fees involved. Because as we speak, there are enough capacities for carrying the national Internet traffic, this type of access is much chipper and can be some-times negotiated separately. RoNIX was a very nice Romanian ISP's initiative of the Y2K's. The basic idea was to establish a Romanian Internet node, where all the local ISP's should be connected. This way, the administration, troubleshooting, prices and services would be very competitive. Unfortunately, higher interests beyond any technical explanation, made the RoNIX members to be fewer and fewer with everyday, many of the national connections to be established these days, over International Internet nodes.
- International Internet is much more expansive, because Romania is not part yet of any major Internet European node. Is unbelievable, but the Internet access for the Romanian market is sometimes 5 to 10 times much more expansive then in United States of America for example and up to 20 times then the one in Japan. This is because we have to pay a lot of money for the International lines in order to "bring" the Internet in our country

from the European nearest Internet nodes (Viena, Paris, Frankfurt, etc.).

My idea was to "treat" these types of traffic independently. For the Metropolitan Internet traffic is very common to negotiate 100 Mbps Internet bandwidth. For the International Internet access, based on the traffic analysis and the clients' requirements it was negotiated a 6 Mbps Internet bandwidth.

The effectiveness of the solution, resides in the equipments used and their actual positioning in the architecture. In order to increase as much is possible the service availability, I have used only redundant configurations: (clusters of firewalls, VPN concentrators [3], proxy and authentication servers, content management switches [4], etc.). Fig. 1 illustrates the entire concept. Let's go in more details:

- Firewalls: Their role was described above. The chosen redundant configuration permits to the hot-standby device to take over "on the fly", without the users to notice this event. This feature is accomplished by using a dedicated interface on both firewall devices (Primary & Standby) that can carry the stateful fail-over information. By using a dedicated DMZ interface on both devices it was reached the highest level of availability, basically all the connections and traffic are present and processed all the time on the standby equipment as well.
- Content Management Switches: Layer 7 ISO/OSI devices give beauty and power to this solution. Practically these devices were programmed to sneak inside the HTTP packet for the "URL" content. In the event of finding at the end of the string something like "*.ro", means that the requested page resides somewhere in Romania (local traffic) and the adopted strategy was to forward this type of inquires to the Metropolitan Internet Proxy Server. This server is happy to engage the requested page over a 100 Mbps line, being a National Internet access. If the requested URL string doesn't contain anything like "*.ro", then the inquiry is forwarded to a shaping router (for the amount of the International Internet Access – in our case 6 Mbps) and handed over to the other Internet Proxy-Server (the International Internet one). Inside the shaping router can be defined different policies for different groups of users in order to guarantee some minimum bandwidth.

Is good to mention about the fact that both of the Content Management Switches are configured in a stateful redundant manner (one of the interfaces being also dedicated to this role). These devices were also programmed to monitor the health state of both Internet Proxy-Servers; In case that any of the servers is experiencing problems, all the traffic destined to the out-of-service one is automatically forwarded to the other, in transparent way.

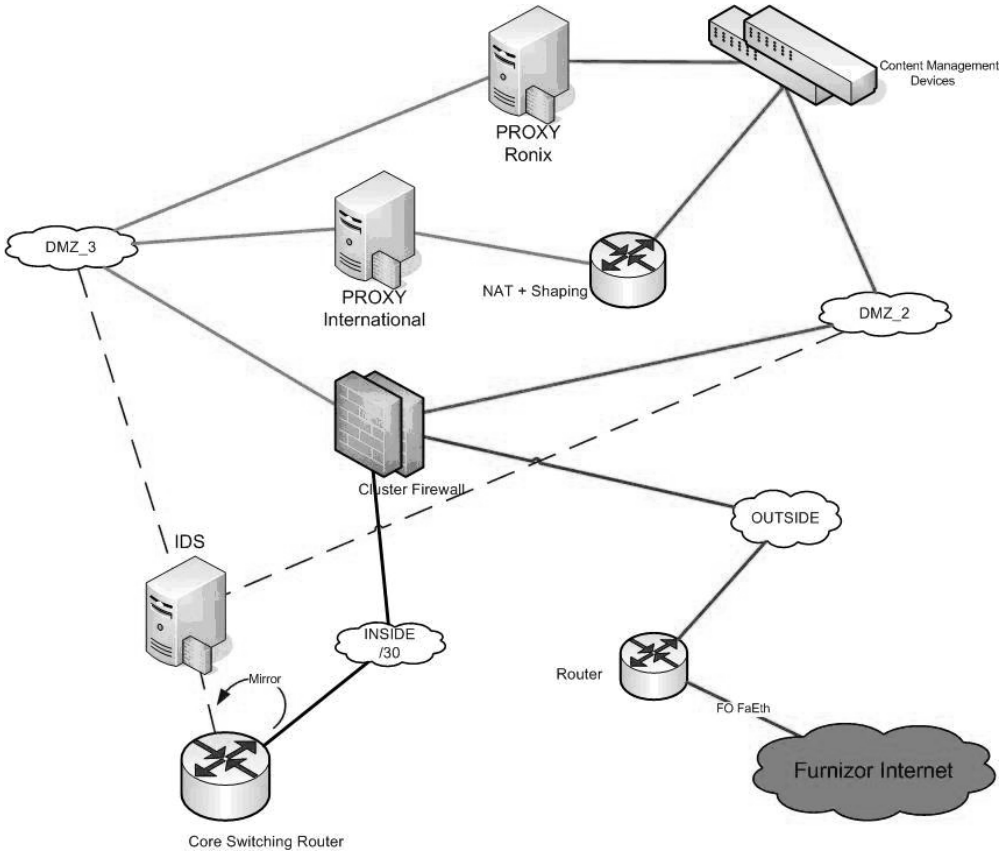


Fig.1. Internet Access Diagram with high availability, budgeting & shaping also available

- It can be seen an IDS [5] device (Intruder Detection System), that "sniffs" the interesting points: Demilitarized and Inside Areas. This supplementary device can monitor and even control by cutting some connections and even changing momentarily the firewall security policies along with triggered alarms. These kind of devices are very effective, only if are correctly programmed, monitored and updated with the latest "signatures"

and policies in order to cope as soon is possible with the new type of threats present along the Internet.

And because we referred a lot to the need of increasing the availability, you should know that any Internet Service Providers doesn't include in their Service Level Agreement more then 97 % for their service. This aspect is normal because of the Internet nature. Everybody provides a limited service by getting you connected, but nobody can guarantee anything as you are there, because nobody owns the Internet.

Because in my case, it was formulated an explicit requirement of the 99% for this type of service, to find a solution was very challenging.
I have contacted RIPE NCC [6] (United States of America), the only organization that can provide Autonomous System Numbers (AS), one of the pre-requisites in order to "announce" yourself in the Internet. The second condition was to obtain from themselves a public IP address class. My idea was to become a small Internet Service Provider myself. This can be accomplished only if you have your own IP public address space, an AS number and a powerful router with Border Gateway Routing Protocol (BGP) [7], [8], [9] activated onto it. These are the conditions if you want to announce by yourself on the Internet. The things are not very simple as it looks. Inside the ISP's world, there are written rules and some only known rules...What is very important is the only accepted language (English), one routed protocol (IP) and just a routing protocol (BGP).

By activating a BGP sessions on my router, I have started a chain reaction inside the whole Internet, that usually lasts about 48 hours. This is how long it takes to the Internet in order to accommodate a new arrival . On the other hand, my router took very serious the shock by "peering" with Internet. In order to fulfill my plan I had activated two BGP sessions. One BGP sessions was peered with another local Internet Service Provider, in order to find out only about the Metropolitan routes (a few tenths of thousands). The other BGP sessions was peered with another Internet Service Provider machine, in order to find out about all the routes available on Internet. The last BGP session was the one that crumbled my router (even if is one of the most powerful machines), because of the approximately 180.000 nets imported in one BGP step. From this moment, I was very careful about my router performances, any "flapping" at this point would trigger one of the unwritten rules on the Internet (to ban yourself out of the Internet). If your are flapping, means that your routing tables is updated very often with the 180.000 destination. Nobody cares on the Internet about your router when is smoking fried of processor intensive, but they are very concerned about their equipments that are doing the same (being in peer with yours).

Coming back to my initial request to perform with Internet Services under an crushing SLA of 99%, being myself an Internet Service Provider didn't help much. Then I have activated another router (same model with the first one) but this time in BGP peer with another Internet Service Provider. The total availability offered by myself, theoretically being within the requested limit. Because of the second Internet Service Provider, my infrastructure became more complex. It was necessary to activate an interior routing protocol (iBGP) between my two full BGP table routers, in order to maintain the shortest path for all destinations. This way, I have gained better connectivity and presence on the Internet then both of my Internet Service Providers. Finally, I have configured on both of my Internet routers, HSRP (Hot Standby Routing Protocol), this time a proprietary solution to gain a high level of availability between the two equipments. This decision, even though it's increasing much further the configuration complexity of the two equipments, represents a very good solution of automatically migration the sessions and the Internet Service Providers in case of one of the routers fails.

Fig. 2 illustrates the upgraded availability concept:

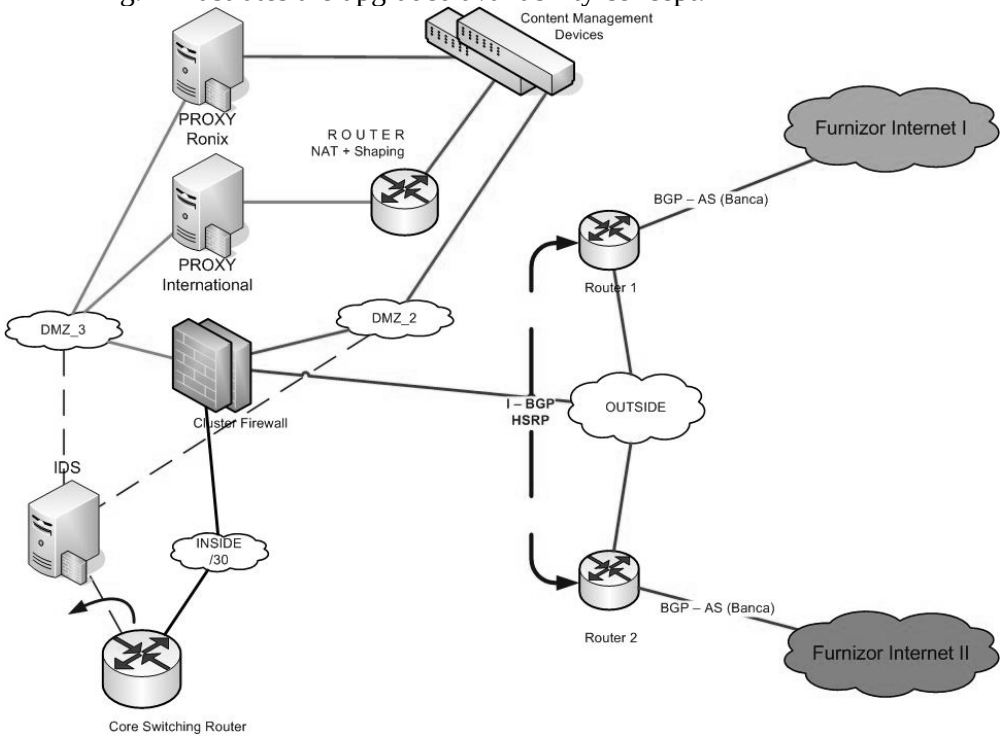


Fig.2. Internet Access Diagram with high availability, budgeting & shaping but with increased availability (presence of two Internet Service Providers)

### 3. Remote access for the mobile users

Over the above proposed architecture, it can be integrated a remote access infrastructure that can provide distant access to the mobile users. This access method more popular each day, provides instant access for the remote users to the local area network resources using different type of media infrastructures (Internet, dial-up PSTN, Wi-Fi, etc.).

The VPN is the acronym for a Virtual Private Network. It was amazing to find out during some of the small-tacks I had, how often the VPN concept is associated with the VLAN one (802.1q). In spite of the fact that "virtual" are both of them, all the similarities ends up here.

The VLAN is used for network segmentation in order to minimize the negative effect of the "multicast" and "broadcast" packets; Also when there is a need of "separating" some user groups data traffic within the same physical network, or when there are delivery special requests for some types of traffic. The "VLAN"-ing is achieved by encapsulating the original packet in a 802.1q standard envelope that includes also a VLAN ID. This encapsulation provided by the second ISO/OSI Layer is increasing the packet size, over the Ethernet standard, so the receiving device must be able to process this "tagged" type of packets.

The majority of typical VPN-related documents define VPN, as the extension of a private network. The definition of a VPN as a dedicated private network based on the existing public or private network infrastructure and incorporating data encryption and tunneling techniques to provide data security, is pretty straightforward. The VPN's, compared with the VLAN's, are born at the third layer of ISO/OSI architecture. The users can create their own IP addressing plan "over" an existing one (public or also private), the respective network being inaccessible from outside.

Starting from these premises, I have elaborated within my company an architecture that can offer to the remote users the ability to access the entire data processing and network infrastructure from abroad. When I'm referring to "mobile users", I'm taking in consideration any employee or third party users having different type of support contracts that can access the "inside" infrastructure based on very strict access policies.

Because we are talking about "remote" access, the solution should be very carefully protected against unauthorized access. Taking in consideration that being abroad, the users can have access to different type of communication channels, there were identified and implemented solutions for three of them:

- Using the Internet;
- Using the Dial-UP over PSTN;
- Using the Wi-Fi [10] devices installed in other company branches.

## 4. Performance analysis of the implemented solution

Being focused in delivering a secure solution, in respect with the confidentiality rules and with the user logging access rules in effect within the company and last but not least having in mind a friendly-user interfaces, I have managed to integrate all the requirements in one architecture.

The solution implies two very powerful VPN concentrators (redundant configuration) and also a software VPN client present on every of our registered mobile users.

The power of this solution resides in the double or even triple authentication method used.

- First level of authentication is provided by the VPN concentrators, through the group name and password provided. This information is configured for the user but not by the user (the password is not known by the user). This measure doesn't allow the user to install another VPN session on another system.
- The second level of authentication is based on a client name and a OTP (One Time Password) provided by a token. The token activation is also PIN dependent.
- The third level of authentication is provided only in case of dial-up connections. In this case the Microsoft dial-up client is authenticating the user once more on a Microsoft Domain Authentication basis.

Parts of this VPN access architecture are also other devices:

- RAS (Remote Access Server). This server is configured with 10 dial-up modems. There is only one phone number (configured as "hunting-head") for all the 10 modems/dial-up lines; The mobile users have their dial-up client configured to dial only one phone number, the PBX does the rest, by choosing the next dial-up line available from the pool of ten. The next step is Microsoft Domain User Authentication, based on the policies involved, the user can get instant "call back" facility or not.
- Secure Access Servers [11]. These devices are configured also in cluster mode for increased availability. They are running specialized applications in charge with the client IP addresses, different security policies, activity logging based on every user security clearance.
- Authentication Servers [12]. These machines are also configured in cluster. There are One Time Password applications that are running on this servers that can provide "Go !" or "Not Go !" conditions for the

Secure Access Servers. The client's token are activated or de-activated also by these servers. Fig. 3 depicts three types of OTP tokens:

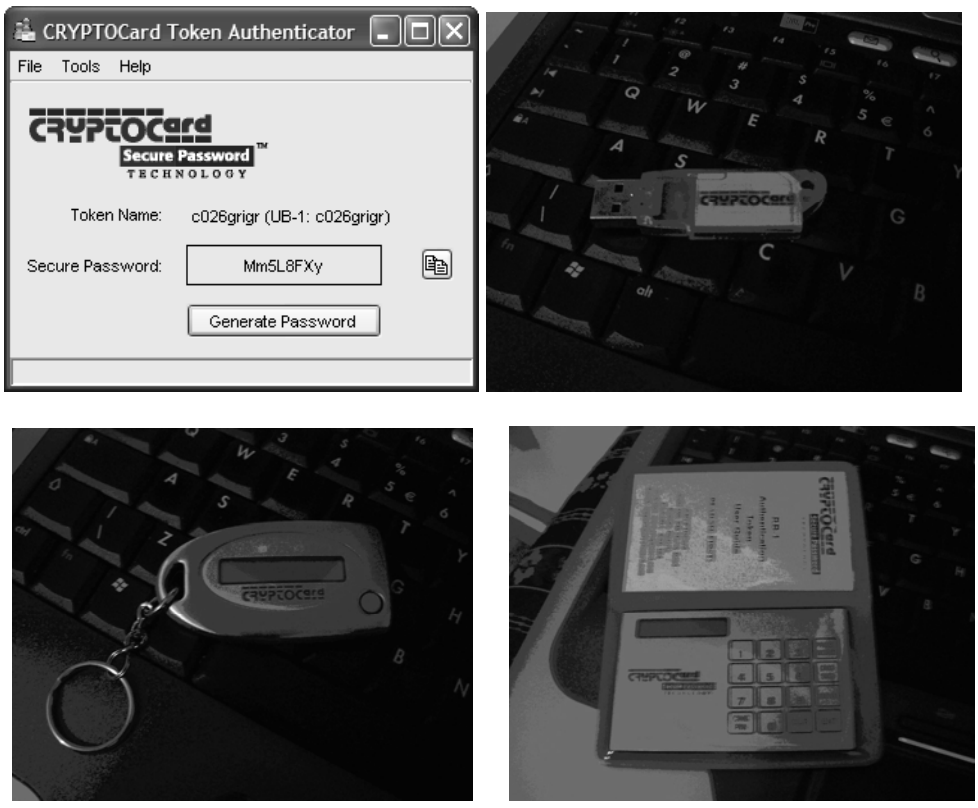


Fig.3. Three types of OTP tokens. USB/software version, key-chain and calculator versions.

- Hot-Spots devices (Wi-Fi – 802.11 a,b,g) that can provide instant connectivity inside company branches. These devices are layer two connected with the VPN concentrators and can be used also by the mobile clients to access the local area network resources using their VPN client. In order to connect to these devices is necessary to be accepted by the Wi-Fi device based on the MAC wireless Ethernet interface; even so there is only limited connectivity (only Internet is provided); In order to gain access to much further devices (located "inside"), the VPN connection is mandatory.

Fig. 4 depicts the integrated solution of Internet distribution and remote access.

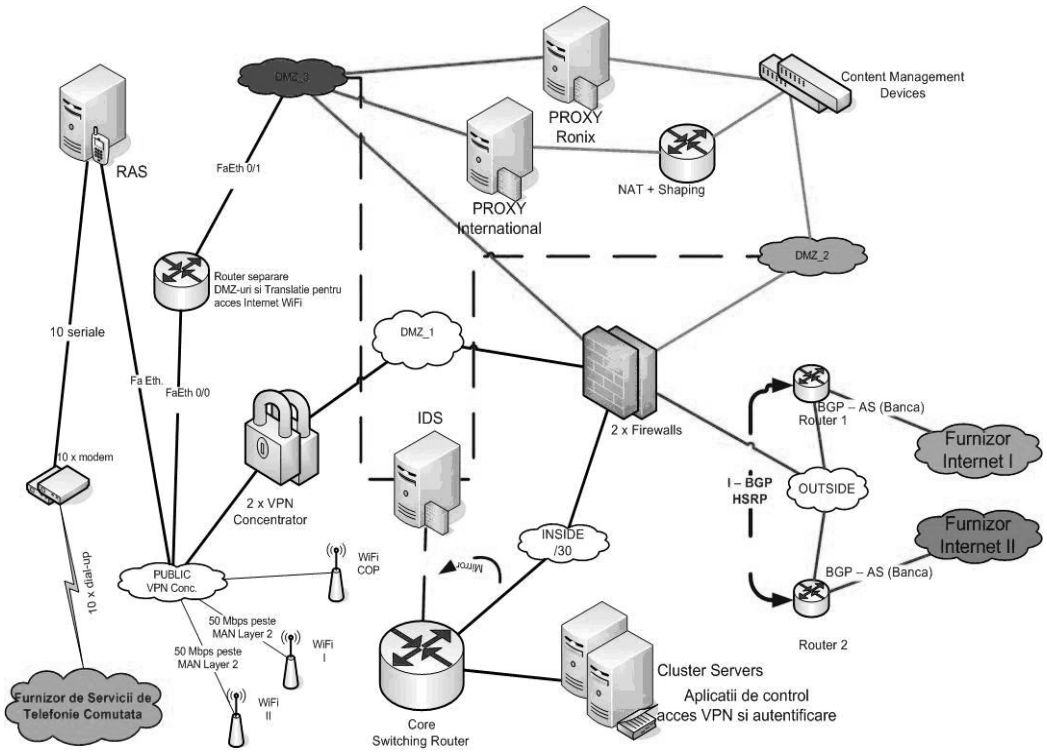


Fig.4. The basic scheme for an advanced and high availability Internet injection along with remote access supplementary services.

Is important to mention that using just two profiles inside the mobile users VPN client (one for Internet and one for Dial-Up/Wi-Fi access), I have created the opportunity to remotely access within the security policies any inside resource in a transparent way. The VPN connection I managed to provide is totally transparent for the mobile users, for them, the connection acts like being connected to the local area network. All the applications drive mappings, IP addressing, DNSes, services, e-mail clients, etc. are running with no need of creating extra profiles. This goal was one of the most important, because the majority of these mobile users are not IT&C professionals.

## 5.Conclusions

I have noticed an increased number of people in our country searching for different ways of connecting to Internet. This became feasible, because nowadays, there are a lot of providers and the infrastructure is better with every day. Because the prices are not as low as for other Internet countries with "tradition" in this area, I've tried to draw a solution that can add value to any medium or large size company and having the means of using the bandwidth in a very efficient way. This is not a theory or an experiment, is based on a real case, it was designed and implemented by me in a financial institution where the security rules and restrictions are more tight then anywhere.

The IT&C technologies are changing as you read these words. The challenges that we are faced are becoming more complicated as we are trying to simplify. The personal development and the deepening of knowledge must be the prime goal of the specialist in this area. The experience is necessary but is not everything. Only the ones that will accept to study forever will prevail.

## R E F E R E N C E S

[1]. *Cisco Systems*. Cisco Secure PIX Firewall Advanced (CSPFA) v7.0. Training January 2006.
[2]. *www.ronix.ro*. September 2001. From 2003, RoNIX is the 25th member of EURO-IX – European Organization of Internet exchangers.
[3]. *Cisco Systems.* Secure Virtual Private Network. Training July 2005
[4]. *Cisco Systems.* Training on Network Solution, IT Security, Enterprise Content Management. Training February 2004.
[5]. *Cisco Systems.* Cisco Intruder Detection/Prevention System Specialist. Training July 2005.
[6]. *Hawkinson & Bates.* Best Current Practice, RFC 1930 - Guidelines for creation of an AS. March 1996
[7]. *Cisco Systems.* Building Scalable Cisco Internetworks. Training 2003.
[8]. *Cisco Systems.* Building Cisco Remote Access Networks. Training 2003.
[9]. *Cisco Systems.* Cisco Internetwork Troubleshooting. Training 2003.
[10]. *Cisco Systems.* Aironet Wireless LAN Fundamentals. Training 2004.
[11]. *Cisco Systems.* Cisco Secure Access Control Server Configuration & Management. Training 2001.
[12]. *CryptoCard Corp.* Crypto-Server Administration. Training 2004.