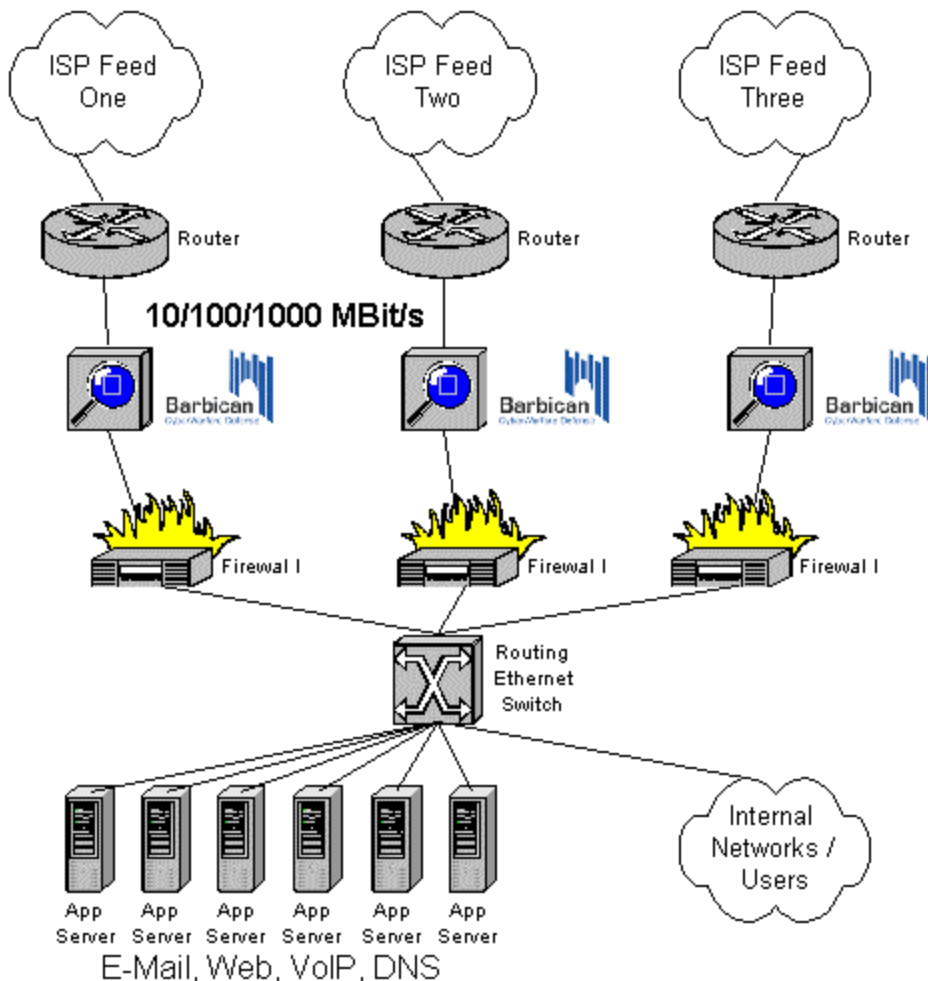


Example 2: Barbican RNP Deployment defending the Perimeter

This document discusses the setup of Melior's Barbican RNP CyberWarfare Defense product to defend your entire perimeter edge towards the outside world.

Deployment: Perimeter Defense: On-Premise



Most medium and large networks are set up in a similar architecture design, following a „best practices“ approach established - until now:

One or more Internet connections are shielded by firewalls, protecting against basic attacks and limiting the number of TCP, UDP, and ICMP ports, on which the outside world can communicate with the systems made available for public access, or on which services using the Internet can communicate (out-bound e-mail, web surfing, Voice-over-IP, DNS, etc).

Penetration Tests probes for vulnerability probing are not intercepted, and the infrastructure is open to attacks and compromises. Each firewall is addressable and runs – like any other device accessible from the Internet – on a TCP/IP stack, which in itself is vulnerable.

With freely available tools, any individual, group, or competitor with malicious intent can determine the exact configuration of the customer's infrastructure (with tools such as NMAP or Nessus), and attack it at will to disable individual components or shut down devices and access to and from the entire infrastructure. A simple stack attack on the firewall will disable all communications instantly.

Barbican RNP defends against these attacks (*please see brochure on „Attack Protection“*), including the PenTest probes (to also protect the on-premise router, it must be installed „upstream“, i.e. on the ISP end of the traffic delivery medium – *please consult our brochure on on-line presence defense*).

As a customer, you will want to eliminate the risks of vulnerability exploitation and direct attacks on your infrastructure by shielding your firewall(s), network devices (switches, routers), and servers, now that **CyberWarfare Defense Solutions** have become available with **Barbican RNP v1.0**.

The benefits are obvious: compare the cost of cost of damages, outages, IT staff usage, and vulnerability exploitation (against which your current security measures do not defend) against the cost of **Barbican RNP** units (or their premium service cost by the ISP).

Benefits for uptime and application availability, such as:

- Web Services
- E-Commerce Services
- E-Mail Services
- Telephony Infrastructure (Voice-over-IP / VoIP)
- Domain Name Service (DNS)
- File Transfer (FTP) Services

Benefits of decreased IT staff costs due to:

- Drastically reduced log sizes in firewalls and Intrusion Detection Systems (IDS) - less IT staff time spent to review logs efficiently
- Reduced need to rebuild firewalls, servers, desktops, and other devices from TCP/IP stack attacks
- Reduced costs from compromises from worm/virus attacks
- Reduction/Avoidance of follow-up costs of vulnerability exploits due to elimination of Penetration Testing for yet-uninfected systems (IT staff time spent to keep up with system patches)
- Budget benefits from improved reporting on valid vs. invalid network traffic

You will find **Barbican RNP** amortizes very quickly.

For additional cost / benefit data, please contact your local reseller or Melior, Inc.'s sales department.

www.dDoS.com