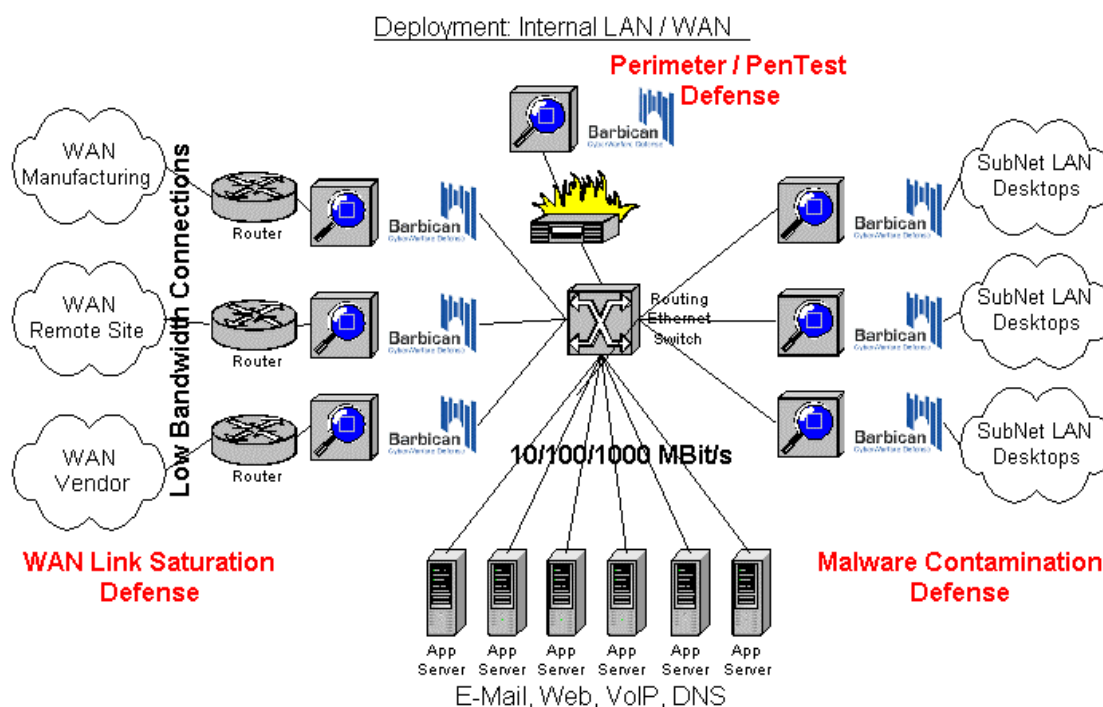


Example 3: Barbican RNP Deployment protecting Internal Networks

This document discusses the setup of Melior's Barbican RNP CyberWarfare Defense product to defend your entire internal infrastructure.



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

User desktop systems share local subnets (LANs), interconnected with Ethernet switches and routers, and providing connectivity to commonly shared resources, such as file- and print servers, e-mail servers, intranet web servers, Voice-over-IP (VoIP) telephony services, and many other applications. External sites (manufacturing, remote offices, privileged vendors) are also often connected via low-bandwidth WAN lines, or through the Internet. The entire infrastructure is typically connected to the Internet via one or more ISP links, and a firewall protects against basic attacks and limits the number of TCP, UDP, and ICMP ports, on which services using the Internet can communicate (in- and out-bound e-mail, web surfing, Voice-over-IP, DNS, instant messaging, etc).

Some high-security conscious sites deploy firewalls also internally between LANs and WANs, and in front of internal application farms, to control access to resources within the infrastructure; however, the cost to deploy and maintain firewalls and their policies is too cost-prohibitive in most cases to actually implement.

Penetration Tests probes for vulnerability probing are not intercepted from external or internal sources, 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 – and the same is true for network devices (switches, routers, VPN gateways), servers, and desktop PCs.

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 from external or internal sites to disable individual components or shut down devices and access to and from the entire infrastructure. A simple stack attack on a firewall, router, or Ethernet switch will disable all communications instantly; attacks on servers and applications will disrupt those equally quickly.

In addition, user desktop PCs are often compromised by viruses, worms, and other forms of malware (studies have shown 40% of desktops in US Fortune 100 companies are compromised), and the malware spreads very quickly across the entire infrastructure, contaminating other LANs, remote sites via WANs, and server farms.

Even simple invalid and „junk“ traffic (such as jabber from malfunctioning network devices; i.e. bad traffic without malice) flows freely across the LANs and WANs, eating up resources. While on a 100 Mbit/s or faster local network this extra traffic is not as much noticeable, it often easily saturates the smaller wide-area network connections, and leads – with growing networks – to costly upgrades of such connections.

Barbican RNP defends against both invalid, non-malicious traffic, as well as against malicious attacks from internal and external sources (*please see brochure on „Attack Protection“*), including internal or external PenTest probes to exploit vulnerabilities in local or remote sites as preparation for targeted attacks.

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

The benefits are obvious: compare the 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 (internal and external access), 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:

- Containment of malware within individual subnets with infected desktop PCs
- Protection of critical LANs and WANs by partial **Barbican RNP** deployment for those networks only
- Drastically reduced log sizes in firewalls and Intrusion Detection Systems (IDS) - less IT staff time spent to review logs efficiently
- Reduced costs 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