

Attack Protection

As an „inline“ device, **Barbican RNP** is designed to deliver on two key purposes:

- ❑ Inspect every single packet and packet stream for validity, to identify invalid traffic and threats, and discard and report on such identified „bad“ traffic
- ❑ As little as possible impact and latency on valid traffic due to real-time inspection, so normal operations are guaranteed

In order to deliver the desired benefits, **Barbican RNP** protects against these attacks:

Connection flood attacks:

The attacker exhausts the target's resources by creating a large number of unused connections to the target.

SYN flood attacks:

The attacker exhausts the target's resources by starting a large number of connection "handshakes" that it never finishes.

Malformed header attacks (TCP, UDP, ICMP):

The attacker attempts to take down, take over or degrade the performance of a target by sending packets whose headers contain invalid data.

Packet fragmentation attacks (TCP, UDP, ICMP):

The attacker attempts to take down the target using packets deliberately crafted to take advantage of faults in certain operating systems or network devices.

Random-source UDP flood attacks:

The attacker consumes the target's network resources by originating a large number of UDP datagrams that appear to come from random origins.

TCP State Machine attacks:

The attacker attempts to take down or degrade the performance of a target by performing protocol actions out of expected order, or in ways that "confuse" the target device's network communication system.

Malformed TCP packet attacks:

The attacker attempts to take down, take over or degrade the performance of a target by sending packets that contain various kinds of invalid data.

These attacks can be geared against specific network devices, operating systems, applications (forinstance: web servers, E-Mail servers, DNS, Voice-over-IP telephony services, infrastructure services such as BGP4) in either broad-scale attacks, overwhelming services or bandwidth pipes, or specifically targeted against known or emerging vulnerabilities.

The determination of vulnerabilities specific to each targeted site and infrastructure is prevented by the **Barbican RNP Penetration Testing Defense** (PenTest), which „cloaks“ the infrastructure against probing attacks.

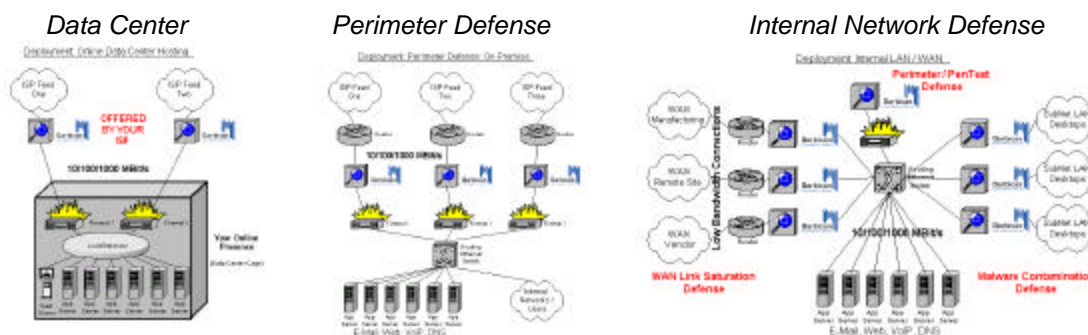
In the initial v1.0 release, **Barbican RNP** is geared to protect against OSI Layer 2 and 3 attacks; however, many attacks targeting applications on OSI Layer 4 and above can be recognized and thus defended against on the lower levels. Melior has several modules in development,

www.dDoS.com

addressing CyberWarfare Defenses against OSI Layer 4 and above attacks, which will become available for easy installation on existing **Barbican RNP** platforms by the customer.

Barbican RNP can be deployed across the entire network infrastructure, to defend against external and internal threats. The **Barbican RNP** product is purposely priced very aggressively, to make wide-spread CyberWarfare Defense affordable to deploy

- ❑ At data center locations to protect your online presence
- ❑ At the external perimeter to protect against external threats
- ❑ At internal network connection points between LAN subnets and between LANs and WANs, to protect against spreading attacks from contaminated PC desktops by containing contamination within local subnets, and to protect against bandwidth saturation on WAN links



See additional brochures discussing the details of various deployment scenarios.

Benefits

- Uptime and application availability during dDoS attacks, such as:
 - Web Services
 - E-Commerce Services
 - E-Mail Services
 - Telephony Infrastructure (Voice-over-IP / VoIP)
 - Domain Name Service (DNS)
 - File Transfer (FTP) Services
- Decreased bandwidth costs during dDoS attacks
- No revenue loss during application request flooding attacks
- Non-Disclosure of Vulnerabilities (no Penetration Testing exploits)
- Decreased IT staff costs due to:
 - Drastically reduced log sizes in firewalls and Intrusion Detection Systems (IDS) - less time spent to review 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 (time spent to keep up with system patches)
 - Budget benefits from improved reporting on valid vs. invalid network traffic

www.dDoS.com