

The Introduction of a new CyberWarfare Defense Layer

Since the invention of firewalls, no major technology development has occurred in computer, network, and application security in the last 10 years. Firewalls came as the first measure to provide some security, after local networks and the Internet were set up to simply provide ubiquitous connectivity with no concern for security. The network devices directing the traffic (i.e. routers) could be configured for some basic security (by way of Access Control Lists – ACLs), but due to very limited CPU capabilities, and an enormous cost in performance, proved to be of little use for security.

The introduction of firewalls then allowed a function of a gateway on the perimeter, to authenticate access, and to restrict the total number of 65,535 TCP and 65,535 UDP communication channels to the few ports actually used. However, this approach provides at best a „Swiss Cheese“, as the ‚open‘ ports – i.e. the most popular ones - remain available for both valid traffic (such as web access, e-mail, file transfer, encrypted traffic, etc) as well as invalid traffic, since firewalls have to pass all traffic without discrimination, and do not have the ability to make decisions, which traffic is valid, and which is not.

In addition, firewalls and all other devices communicating with a TCP/IP protocol („stack“) are addressable, and can be directly attacked themselves. By sending malformed data, non-complying with the established protocol rules, or carefully crafted to operate outside established boundaries, every single one of such devices can be very quickly eliminated („crashed“), thus disrupting communications and shutting down the availability of resources.

See also Melior's Brochure: „Is A Firewall Enough?“

Penetration Testing: Mapping Vulnerabilities

Additional tools allow for an exploitation of configuration, thus mapping the infrastructure, and providing an exact catalogue of deployed hardware, software, and its configuration, which in turn can be easily used to determine the weak points („vulnerabilities“) and to exploit those in targeted attacks. These tools are freely available and very powerful („Penetration Testing Probes“). Programs such as NMAP or NESSUS will provide such maps of an entire architecture design, and in addition even rate the difficulty for compromise.

Such vulnerabilities can then be exploited even further, with distributed Denial-of-Service (dDoS) attacks.

What is a Denial-of-Service (DoS) attack?

Broadly defined, a DoS attack seeks to overwhelm the capabilities of the targeted site, either from the outside (the Internet) or from the inside (internal systems), with the intention to disrupt (deny) service – by disabling („crashing“) the targets or by sending so much traffic, that the target is no longer able to respond.

These attacks come in many different flavors. They can be very small, sending a short burst of only a few malformed packets (such as in „shrew“ attacks, „synk4“, or „synk5“ attacks) against just one critical system, representing a key, single-point-of-failure component (such as a firewall), and almost instantly taking it down, thus shutting down access to and from all systems behind this device.

The attacks can also be very large. The concept of „bot-networks“ has matured, in which a large number of computers on the public Internet are quietly (without the knowledge of the owner) compromised, and thus listen to a single command from a „bot-net-operator“ to send attack traffic against a particular target simultaneously with thousands (or even millions) of other computers. These attacks are usually carefully crafted, and hide the IP address of each such computer, pretending with each individual packet sent to come from a different IP address (this function is called „sender address spoofing“). Since this form of DoS attack comes from so many distributed systems, it is called distributed Denial-of-Service, or dDoS, attack.

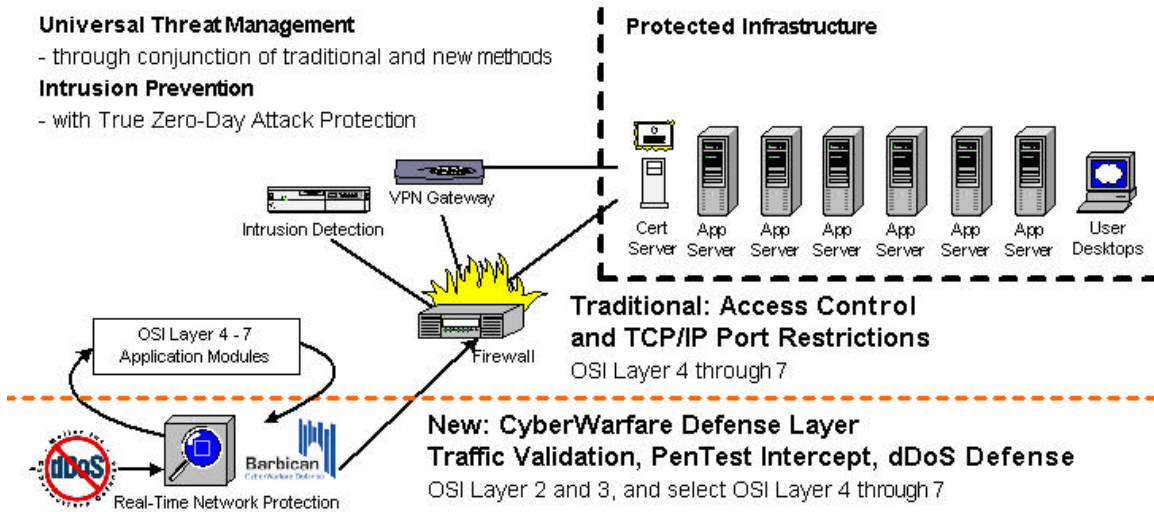
With existing security measures, the attacked site has no means to determine which part of the incoming bandwidth is valid traffic from regular visitors with their correct IP addresses, and which part is invalid, coming from „spoofed“ computers. Consequently, the attack is successful, usually works immediately, and keeps the targeted site offline, until a central command is issued to all the systems in such a „bot-net“ to cease the attack.

This method is virtually risk-free to the attacker, as it is technically impossible to identify all the participating computers in a „bot-net“, and trace back from those to the operator, issuing the single attack and cease commands. Even if that were possible, the attacker is likely located in a different jurisdiction than the targeted site, thus excluding any reasonable possibility to take appropriate action.

Distributed Denial-of-Service attacks have become increasingly popular in the last years. They are used by organized crime groups to extort large sums of money from e-commerce services (for example, virtually all online betting sites in the UK are paying extortion fees after several large attacks), they are used by political groups (news sites have been shut down for extended periods of time), and the risk of terrorists attacking entire countries with the desire to disrupt that countries' Internet commerce, communication channels, and economy is another great concern to Government officials.

The Introduction of a new CyberWarfare Defense Layer

First major technical advancement in network security since firewall introduction



www.dDoS.com

In order to defend against these malware, PenTest, DoS, and dDoS attacks, the existing security measures need an additional layer: a layer, which inspects all traffic prior to reaching critical systems, and eliminates all (sic!) invalid traffic.

This functionality, now for the first time available with Melior's **Barbican RNP**, goes deeper, to Layer 2 and 3 of the OSI model, while inspecting traffic on application Layers 4 and above for validity as well.

- ❑ **Not detectable** on the network – so it cannot be addressed itself, and thus not be compromised (no MAC or IP address)
- ❑ **„Inline“ Appliance:** the only viable approach to inspect **all** traffic first, and not let a single bad packet pass, requires the CyberWarfare Layer to sit „on the wire“. Any other approach, observing traffic flowing through other devices, does not have sufficient time to react, and thus – by design - has to let invalid (or „bad“) traffic pass, while it determines if action needs to be taken.
In addition, the Barbican RNP approach as an „Inline“ device requires no changes to the various existing environments, no additional switch ports, or any re-engineering of the protected architecture. Since this is a single point of failure, the CyberWarfare Defense layer must be protected against failures, thus have as little moving parts as possible, and come with extensive protection against failure (at least the same level as other critical single-points-of-failure devices)
- ❑ **Real-Time Defense** is mandatory to this layer to function well. Valid traffic must pass the CyberWarfare Defense layer with a minimum of latency, not to exceed 10 milliseconds, while all invalid and attack traffic is discarded instantaneously.
- ❑ **True „Zero-Day“ Attack Defense** is another mandatory requirement. ALL other security devices use a library or „signature“ data base to compare observed traffic against, such as firewalls („policy definition“), Intrusion Detection Systems („signatures“), anti-Virus software („Virus Libraries“), and anti-Spam software (a variety of solutions, from dictionaries, blacklists, heuristic definitions, etc).
This approach can only recognize „known“ – previously observed – forms of attacks, and by design, the growing size of such definitions (which need to be constantly updated) make the comparison process increasingly slow, before any counter measurements can be taken. New and modified forms of attacks, deviating from those pre-defined, known attacks, will pass the security device without challenge.
The CyberWarfare Defense layer must not „know“ any attacks, and look at every single packet with the ability to decide if it is valid or invalid: it must operate **„signature-free“**; thus providing true „Zero-Day“ attack defenses.
Barbican RNP is the first such product: it's patented technology provides a „Truth Table“, which inspects all traffic for validity without any comparison process, and acts in real-time to pass on the valid traffic, while discarding (and reporting on) the invalid traffic.
For details on defense capabilities, please see Melior's brochure „Attack Protection“
- ❑ **Penetration Testing Defense** is another critical component of the CyberWarfare Defense layer. All vulnerability and mapping probes must be intercepted prior to reaching any device on the network: if a firewall were to perform this function (or any other addressable device), it would still minimally disclose the type of this device, thus opening the opportunity to address, attack, and disable the device.
Barbican RNP intercepts and responds to such probes, increasing the difficulty level for compromise by adding partial (probed port is reported as „open“, but no other information is provided) and random (so Barbican RNP itself cannot be catalogued) data to the response. In turn, it allows other, existing security technologies, such as Intrusion Detection Systems (IDSs) to function better, by „tuning“ the device to listen for such

- Barbican RNP PenTest responses and trace the source of the probe for appropriate counter-measures.
- ❑ **Ease of Deployment** is important to deploy the CyberWarfare Defense layer across a variety of infrastructures, with or without skilled IT Security staff present, as well as to achieve instant protection. If it were to require a lengthy „learning“ period to gain information of „normal“ operations, it would deploy old bandwidth throttling technology, and be inefficient to provide instant protection. Barbican RNP works in a „Plug & Protect“ mode: as soon as the CyberWarfare Defense device is plugged in, it protects instantaneously.
 - ❑ **Affordability** is key for wide-spread deployment of the CyberWarfare Defense Layer, so access to this technology is open to every single organization, whose systems are critical to its infrastructure, regardless of the available security budget. Barbican RNP is aggressively priced to provide this affordability in a variety of deployment options for the CyberWarfare Defense Layer.

With the availability of Melior's Barbican RNP, a CyberWarfare Defense Layer is available for the first time since firewalls were invented, providing a major step forward in the mix of security measures towards a unified threat management – and offering better options to comply with legal network- and application-protection requirements.

300 million users, who were already successfully protected against dDoS attacks by Melior CyberWarfare Defense technology, attest to the validity of the CyberWarfare Defense layer.

Additional testimonials demonstrate the benefits of PenTest defense, reduced processing loads on firewalls as a result, reduced log sizes, and additional financial benefits in the reduction of IT staff resources.

Melior, Inc.
CyberWarfare Defense Solutions