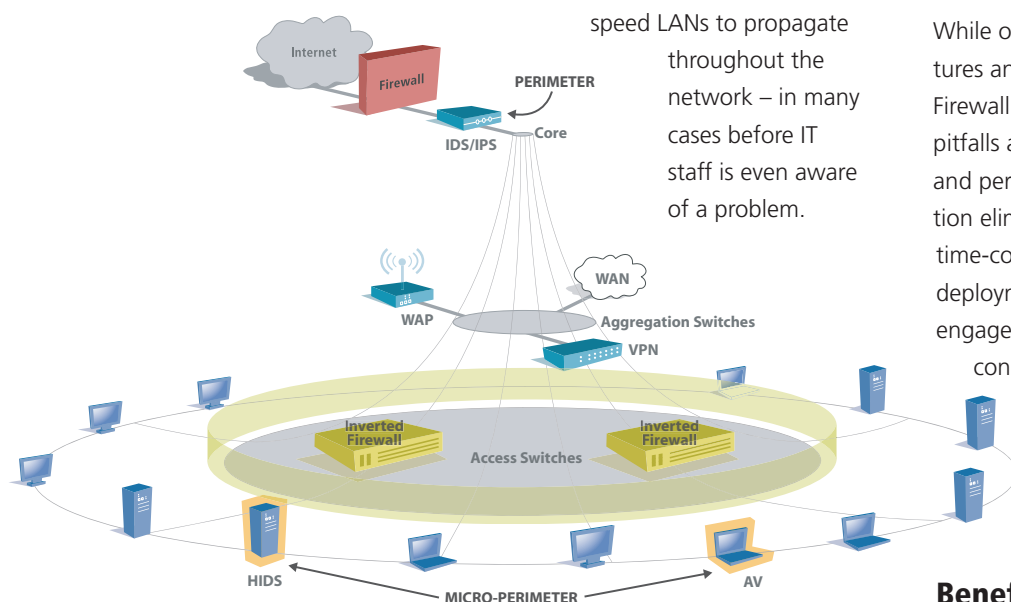


## Mirage Networks Inverted Firewall

The first network security appliance designed to actively defend the network interior.

Traditional security approaches rely on network perimeter and host-based “micro-perimeter” barriers to keep networks safe. Unfortunately, the most damaging and costly exploits are those that target the area between these two security boundaries – the network interior. In recent history, malicious traffic has been leveraging mobile computers, VPN connections, partner extranets, misconfigured firewall rules and other perimeter “holes” to completely bypass traditional security roadblocks. Once inside, this malware takes advantage of high

speed LANs to propagate throughout the network – in many cases before IT staff is even aware of a problem.



The Mirage Networks Inverted Firewall is the first network security appliance designed to actively defend the network interior, stopping network threats before they cause widespread damage. This new layer of security complements existing investments in firewalls, IDS/IPS, AV and HIDS/HIPS by identifying, slowing and containing unknown threats other solutions cannot address. Most importantly, threats are eliminated with pinpoint accuracy, creating no interruption to business-critical traffic and helping to maintain business continuity.

The Inverted Firewall’s comprehensive feature set offers the lowest possible total cost of ownership for interior security, since the solution has:

- No signatures to maintain
- No agents to deploy/manage
- No source of latency
- No single point of network failure
- No required network rearchitecture
- No unreliable heuristic-learning mode

While other security solutions rely heavily on signatures and require in-line deployment, the Inverted Firewall’s unique technology allows it to avoid these pitfalls and eliminate the associated maintenance and performance costs. Its behavioral threat detection eliminates signature updates without issuing time-consuming false positives. Its virtually in-line deployment allows the appliance to actively identify, engage and mitigate threats through a simple connection to a switch port. This out-of-band deployment allows the appliance to be installed and configured quickly and operate without negatively impacting network traffic.

### Benefits

With the Inverted Firewall, IT professionals have access to new levels of visibility and enforcement on internal networks. This control translates directly into benefits for the business, including the ability to:

- Maintain business continuity
- Eliminate the cost of worm damage
- Reclaim network performance lost to reconnaissance
- Reduce exploitation of network misconfigurations

## Maintain Business Continuity

Because rapidly propagating threats can overtake networks in minutes, interior security solutions are not only a requirement for protecting network resources – they are essential in preventing the loss of business productivity. Therefore, it is critical that these solutions are not in and of themselves hurdles to network productivity. The Inverted Firewall, with its virtually in-line deployment, allows traffic to flow freely, surgically isolating only malicious activity and enabling the rest of the business to function as normal.

## Eliminate Worm/Virus Damage

As malware developers create faster, smarter and more destructive worms, companies are at greater risk than ever before when vulnerabilities are discovered. Analysts have stated that on average, each malicious code incident costs between \$213,000 and \$475,000. The Inverted Firewall, with its ability to identify and automatically contain unknown worms and viruses before they spread, enables IT staff to avoid costly cleanup – or worse – widespread destruction of intellectual property.

## Reclaim Network Bandwidth

Unwanted reconnaissance activity can constitute up to 30% of network bandwidth. The Inverted Firewall can identify and block this reconnaissance, increasing network performance.

## Reduce Exploitation of Misconfigurations

The Inverted Firewall can identify when and where hacker reconnaissance has found holes in perimeter security solutions. In many installations, customers immediately identify traffic exploiting misconfigured firewall rules.

## Features

The Inverted Firewall has three main feature sets – HyperDetection, ActiveDeception and Surgical-Defense – that can be individually configured to give customers the exact level of threat visibility and control necessary for securing their internal networks.

## Day-zero Threat Identification

With **HyperDetection**, the Inverted Firewall watches network traffic, identifies threats and provides notification to IT staff. Its behavioral detection does not require signatures or involve complicated heuristic-learning processes. Threat detection is accomplished with:

- An Early Warning System that utilizes unused IP address space to identify scanning
- A Threat Assessment Engine that provides unparalleled identification of unknown threats

## Attack Intervention & Misdirection

Once threats are identified, the Inverted Firewall uses **ActiveDeception** to mislead and slow them, giving IT staff time to intervene. Configurable elements of this feature include:

- Virtual Decoys with realistic OS and IP personas that provide false data to reconnaissance scans and camouflage real network devices
- Hacker-jamming techniques that use Virtual Decoys to respond to attack threads, preventing them from moving on to real devices

## Automated Threat Containment

The Inverted Firewall's **SurgicalDefense** capability provides the most aggressive level of threat engagement, allowing customers to set automated threat response actions. The appliance can isolate any source of malicious traffic, preventing it from spreading rapidly propagating threats like Slammer, Blaster or Mydoom throughout the network. Because the Inverted Firewall is deployed out-of-band, it contains attacks without interrupting the flow of normal traffic.

## Deployment

The Inverted Firewall's virtually in-line design allows it to reside on the interior network without introducing latency or requiring high-cost ASICs processors. It installs close to the endpoint devices that need protection, allowing it greater ability to see and stop threats that come onto the network.



**Mirage Networks**  
5001 Plaza on the Lake  
Suite 101  
Austin, TX 78746

**Phone:** 512.874.7800  
**Fax:** 512.874.7806

**www.miragenetworks.com**  
sales@miragenetworks.com

© Copyright Mirage Networks.