



# Mirage Networks® CounterPoint™ Rules

Defending the Network Interior™



Mirage Networks CounterPoint provides built-in rules, each designed to detect and mitigate a certain type of behavior. Together, these rules will detect threat behavior arising from the most common methods used to breach networks. CounterPoint comes preconfigured with these rules, which can be modified to reflect network parameters and needs.

### No False Positives.

“Gartner clients that have deployed Mirage’s product report simple installation and effective security...without false actions during normal activity.”

– Gartner Cool Vendors in Security, 2005



### Rule Set A: Threat Propagation

These rules focus on with whom a sender is communicating and how often. CounterPoint tracks traffic to unused IPs and provides deception technology that leverages those unused IPs and patent-pending deception technology to slow and block the would-be attacker. This rule set consists of 4 subsets:

#### 1. “Unused” Rules

An “unused” machine can be a decoy machine, set up specifically to catch would-be attacks, or it could simply be an IP that is connected to the network but is not in use. Communication with an unused machine is considered hostile behavior by CounterPoint, as it indicates the sender is attempting to initiate contact with a machine that isn’t there. CounterPoint enables the setup of decoys with appropriate personalities, which generate a response (for example, a Windows personality generates a Windows-type response).

#### 2. Too Many Used

This rule looks for communication with too many real machines on a network in a given period of time.

#### 3. Too Many Unprotected

Network administrators can set an upper limit on the number of simultaneous communications allowed between used devices on a network, and can also choose not to protect a network segment. Legitimate users generally hit far less than 100 IPs a day. Malware spreaders hit thousands. When a machine initiates communication, this rule detects if it has made contacts to too many unprotected IPs.

#### 4. Too Many External

An external device is any device on a different, protected VLAN or Layer 3 separated network. Network administrators can set an upper limit on the number of simultaneous communications allowed between separate, protected VLANs, to detect if a machine has been making too many contacts to too many external IPs.

### Rule Set B: Bad Packets

When one device initiates contact with another, it sends TCP packets to determine if a connection can be established. Certain packets only exist to commit reconnaissance, and are identified by these rules by their violation of protocol standards.

### Rule Set C: Mail-Related

Worms are often propagated via email. When an email is sent, the sending machine does a “DNS Lookup” in which it translates the send-to name to that machine’s IP address. Therefore, only mail servers should perform a DNS Lookup – when any other machine performs a DNS Lookup, it is likely malicious behavior. For worms to be successful, they must be sent to the greatest number of hosts possible. Non-legitimate users will set up mail servers on their own machines. This rule enables the differentiation between mail servers talking to each other and clients sending to mail servers, for the detection of rogue mail servers.

### Rule Set D: Reconnaissance

These rules catch cyber criminals who attempt to find a chink in the armor via a ping flood - trying to find machines by flooding a network with as many packets as possible, as quickly as possible and/or a port scan - trying all the different services on identified targets, similar to a burglar trying all the doors and windows on a house.

### Rule Set E: Spoofing

These rules catch and stop spoofing, in which the initiator changes the appearance of a packet’s source sends packets to make it seem that the sender is someone else. Spoofing can result in a Denial of Service attack.

