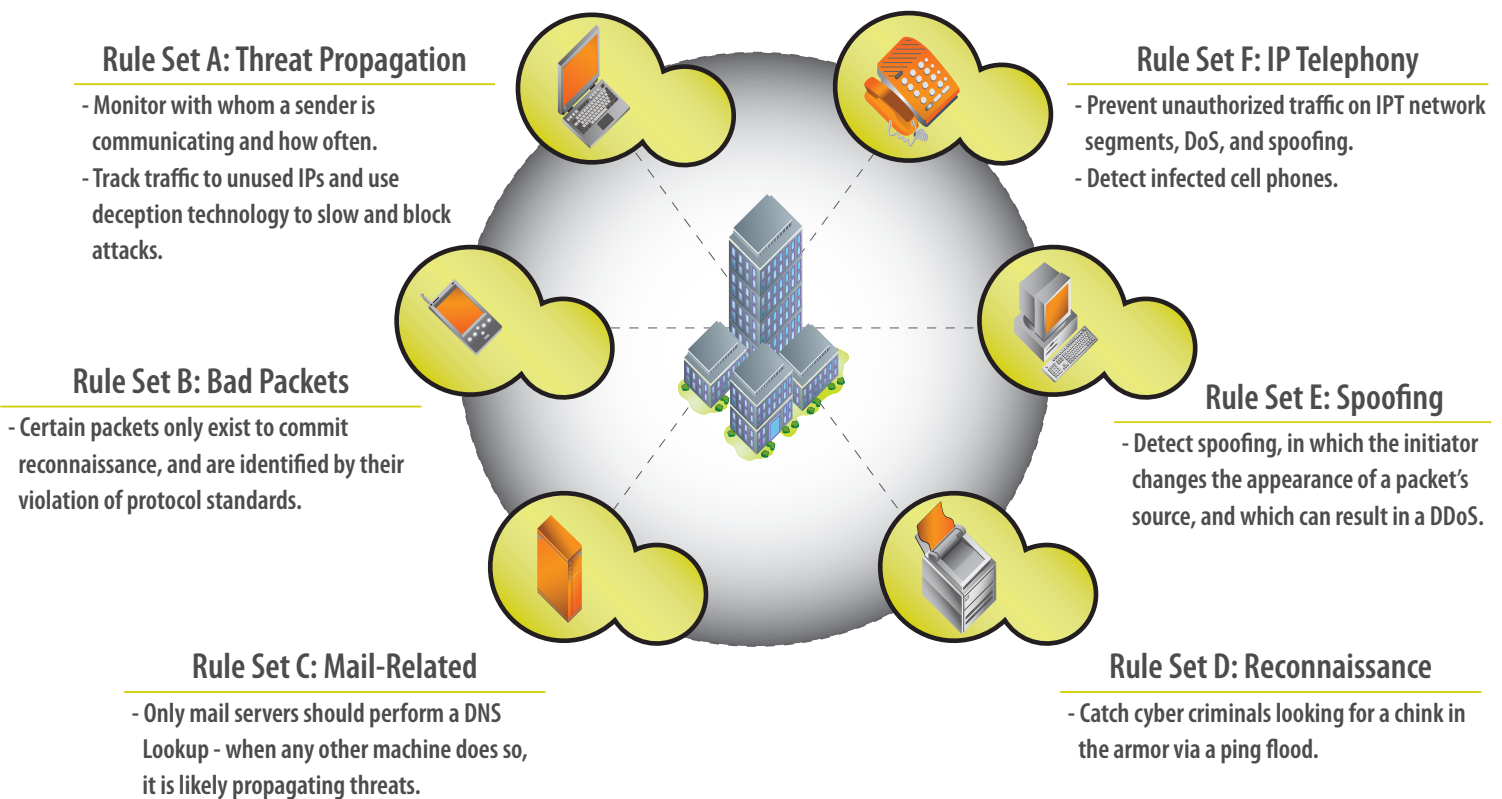


The core of Mirage NAC™ is a behavioral rule set:
six categories of rules, which detect behavior that is indicative of an
attack, either internal or external.



Behavioral Rule Scenarios

EMAILED THREATS

Many worms spread by downloading an SMTP mailer onto the device they are infecting to enable a rapid spread. A user's PC or laptop will generally send out less than 50 emails in one day; Mirage NAC's behavioral rules can identify excessive email traffic as potentially threatening, so the offending device can be quarantined.

IP TELEPHONY THREATS

When setting up an IP telephony network, IT should be able to prevent specific device types from entering areas designated for IP telephony devices. For instance, if a Windows® device attempts to access IP telephony network assets, Mirage's rules detect this traffic and can block it, stopping a potential threat in its tracks.

You Can't Control People. Control What's On Your Network.™

About Mirage Networks

Mirage Networks is an Austin, Texas-based network security company dedicated to delivering real world, complete network access control solutions, serving the enterprise through a strong channel of resellers, original equipment manufacturers and managed security service providers. Mirage solutions ensure a user-friendly and IT-friendly experience that never forces a compromise between business objectives, effectiveness and usability. The company's passion for innovation has paved the way for the development of patent-pending behavioral technology that consistently wins industry awards. Contact us today to learn more about the industry's only self-contained network access control solution.

Contact Us Today:

Mirage Networks
6801 North Capital of Texas Highway
Building 2, Suite 200
Austin TX 78731

phone: 866.869.6767

fax: 512.874.7806

email: info@miragenetworks.com

web: <http://www.miragenetworks.com>