



How OKENA Is Positioned Favorably vs Distributed Firewalls

Distributed firewalls, DFWs, deploy firewall functionality directly on servers and desktops. While personal firewalls are often designed for home use, a DFW must contain a management capability to make it suitable to enterprises. In addition to traditional firewall functionality, many of today's DFWs also include combinations of IDS and

content pattern matching features. Leading distributed firewall vendors are Sygate, InfoExpress and F-Secure.

Distributed Firewall strengths:

?? DFWs do protect against internal and external users.

?? DFWs allow IT to specify addresses and ports to protect individual servers and desktops from inappropriate network use.

?? DFWs have a management capability designed for the enterprise.

Distributed Firewall limitations:

?? DFWs do not have application visibility. Thus they cannot distinguish between a production web server or a Trojan horse use of Internet ports and protocols.

?? DFWs may require significant resource to configure and maintain address and port settings.

?? DFWs do not protect against damage to the file system or application data once the network packet is passed to the operating system.

OKENA StormWatch strengths:

?? OKENA goes beyond DFW in preventing damage from file and network attacks that Pattern Matching technologies cannot detect.

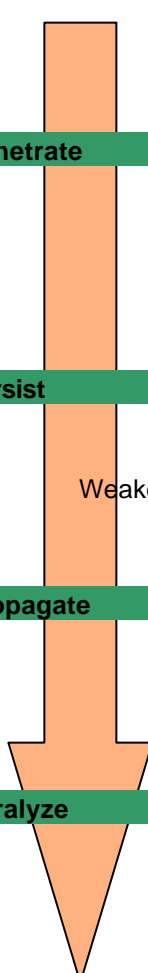
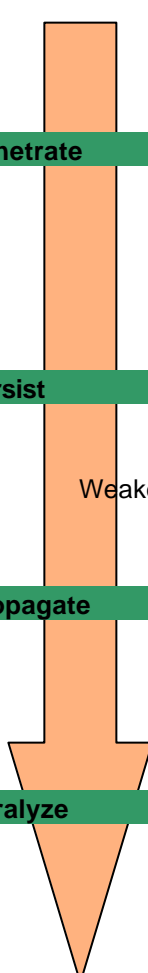
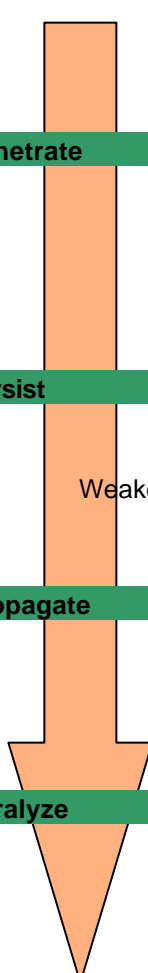
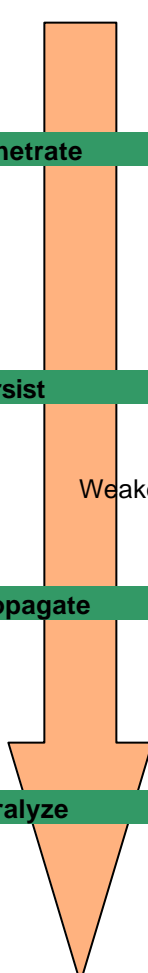
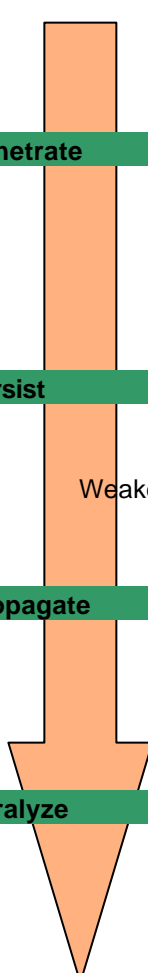
?? OKENA's customizable rules allow IT to control network access by application.

?? OKENA provides a scalable administration model designed for the enterprise.

?? OKENA's distributed behavior enforcement proactively detects POA sweeping.

Bottom Line message:

Distributed Firewalls solve only a small part of the security problem. OKENA's behavior enforcement technology goes far beyond DFW in protecting servers and desktops from attacks. OKENA includes basic DFW features and also prevents damage based on correlating file and network operations.

Lifecycle of an Attack		Okena	DFW
Probe			
	Ping Addresses	Yes	Yes
	Scan Ports	Yes	Yes
	Guess Passwords	X	X
	Guess Mail Users	X	X
Penetrate			
	Mail Attachments	Yes	Yes
	Buffer Overflows	Yes	Yes*
	ActiveX Controls	Yes	X
	Network Installs	Yes	X
	Compressed Messages	Yes	X
	Backdoors	Yes	Yes
Persist			
	Create New Files	Yes	X
	Modify Existing Files	Yes	X
	Weaken Registry Security Settings	Yes	X
	Install New Services	Yes	Yes
	Register Trap Doors	Yes	X
Propagate			
	Mail Copy of Attack	Yes	X
	Web Connection	Yes	X
	IRC	Yes	Yes
	FTP	Yes	Yes
	Infect File Shares	Yes	X
Paralyze			
	Delete Files	Yes	X
	Modify Files	Yes	X
	Drill Security Hole	Yes	X
	Crash Computer	Yes	X
	Denial of Service	Yes	X
	Steal Secrets	Yes	X

Preventative Security Provided During an Attack