Target Customer Segments

Cisco Firepower Threat Defense (FTD) Next Generation Firewall (NGFW) complimented with Red River's 24x7 managed services support gives customers peace of mind for their perimeter security, remote-access VPN solutions, or extranet connectivity. The highly adaptable NGFW scales to business needs while providing threat defense, malware detection, and compliancy to the organization.

SLED

The FTD provides a wide range from desktop units to large throughput rack-mounted units, and Industrial firewall units available with DIN rail systems. The managed firewall portfolio provides a solution for municipalities, utilities, and traditional enterprise environments. The FTD provides a way to secure campus users, data centers, OT environments, and SCADAs. Due to the distributed nature of SLED environments, a scalable FTD solution, overlaid with the Cisco Defense Orchestrator or Firepower Management Center allows for common security policies across all perimeter devices.
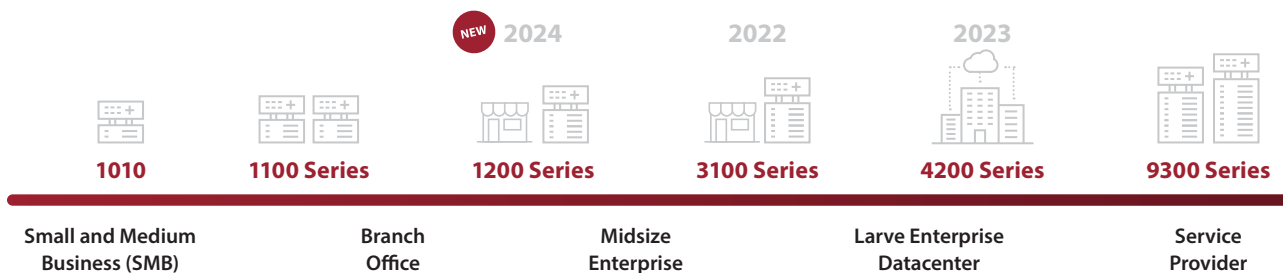
Mid-Range Enterprise

The NGFW capabilities of the FTD provide threat and malware detection to campus and data center networks. In addition to the Remote Access and Site to Site VPN capabilities, the FTD provides clientless Zero Trust access, providing authentication and authorization to applications behind the protected firewall. The FTD provides NGFW capabilities with threat and malware detection, leveraging AI/ML to detect threats against the Talos Threat feed.

Cisco Talos Empowers firewalls with AI/ML Intellegence

- 550B security events/day
- 9M emails blocked/hour
- 2,000 new samples/minute
- 2,000 domains blocked/second

NEW 2024		2022	2023	
1010	1100 Series	1200 Series	3100 Series	4200 Series	9300 Series

1010	1100 Series	1200 Series	3100 Series	4200 Series	9300 Series
Small and Medium Business (SMB)	Branch Office	Midsize Enterprise		Larve Enterprise Datacenter	Service Provider

TECHNOLOGY DECISIONS AREN'T BLACK AND WHITE. THINK RED.

Service Packaging

Red River Managed Firewall Solution Includes:

+ NGFW Redesign
- Identify business objectives and how the NGFW integrates with these goals.
- Evaluate existing policies and rulesets for areas of optimization.
- Explore net new NGFW features that may benefit the organization.

+ Implementing the solutioned NGFW
- Rack and cable the NGFW solution.
- Baseline and configure the NGFW.
- Integrate into the existing network infrastructure.
- Provide day 1 on-site support and follow on remote support.

+ Ongoing system maintenance including patching and updates

+ Periodic configuration review for efficacy of security policy

+ Traffic reports and analytics

+ [Optional] SOC service overlay

Cisco Firepower Threat Defense provides a strong platform for security observability and enforcement, and Red River helps organizations realize that potential. As part of the Managed Firewall Service Red River provides, our consultative engineers will meet with the customer to discuss business intents and security policy to map these facets to the NGFW.

Red River's white glove installation services aim to provide a fully executed solution as least disruptive to the environment as possible. Red River leverages intricate pre-deployment designs to deliver the solution to the customer, ensuring full communication across the process. At the closure of the deployment, Red River conducts a thorough knowledge transfer to inform the staff of the technology and how it is mapped to the organizational goals.

Upon completion, Red River turns the solution to the managed services where the organization gains 24x7 support from the Red River Service Desk and NOC teams. Ongoing maintenance, patching and upgrades are performed to ensure the Managed Firewall Solution is compliant and capable of new features and functionality. Red River offers periodic review of policy and configuration to discuss the efficacy and security of the NGFW solution. Traffic reports and analytics provides the organization with data points and KPIs to aid businesses decisions.

Red River