Red River

cisco Partner

JULY 25, 2024

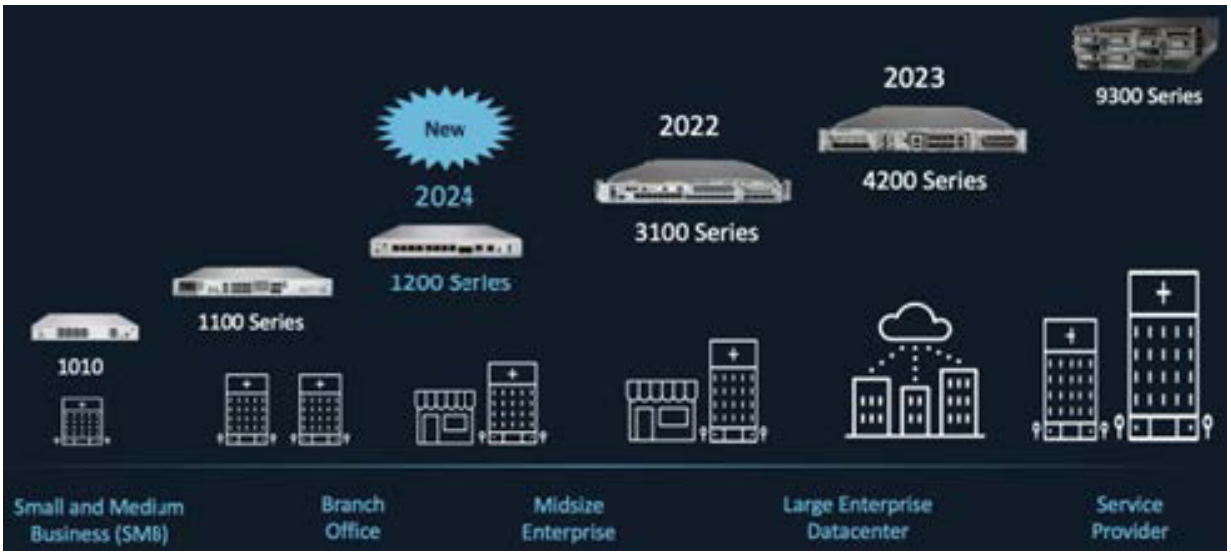
RED RIVER MANAGED FIREWALL

TABLE OF CONTENTS

TARGET CUSTOMER SEGMENT

Cisco Firepower Threat Defense (FTD) Next Generation Firewall (NGFW) complimented with Red River's 24 X 7 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 compliant to the organization.

FIGURE 1



A. 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.

B. 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.

Red River Managed Services provides peace of mind to your investment with 24 X 7 monitoring and management, providing customers new innovations combined with Red River expert-level knowledge.

FIGURE 2

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.
    - URL filtering, threat protection, authentication, authorization, policy, and DLP
    - Mapped to user, application, or identity-mapped traffic
- 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.

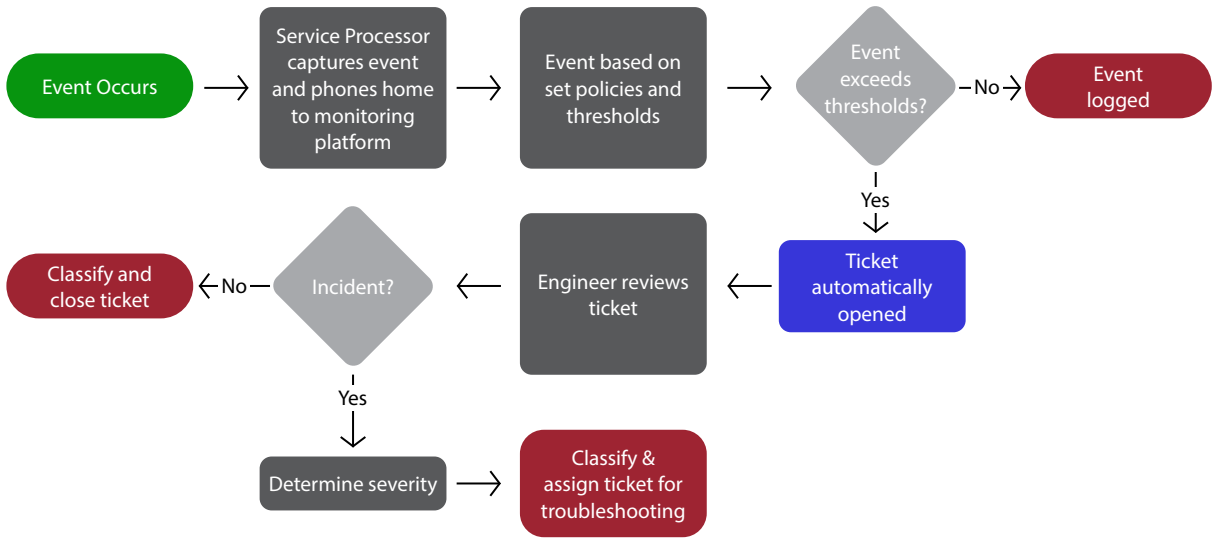
Red River's white glove installation services aim to provide a fully executed solution as least disruptive to the environment as possible. Red River leverages intricate pre-deployment designs to deliver the solution to the customer, ensuring full communication across the process. At the closure of the 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.

A. Monitoring

Red River uses industry-leading tools such as LogicMonitor for our monitoring platforms to process events triggered by the supported configuration items. The figure below depicts the overall workflow, which consists of multiple policies, automation, and SOPs. If included, management of events from Firepower and LogicMonitor will follow a similar workflow once the source generates a ticket.

FIGURE 3: EVENT MANAGEMENT WORKFLOW



MONITORING

RRMS establishes policies and thresholds for the following standard monitors:

Availability

Latency

Memory

Swap

CPU

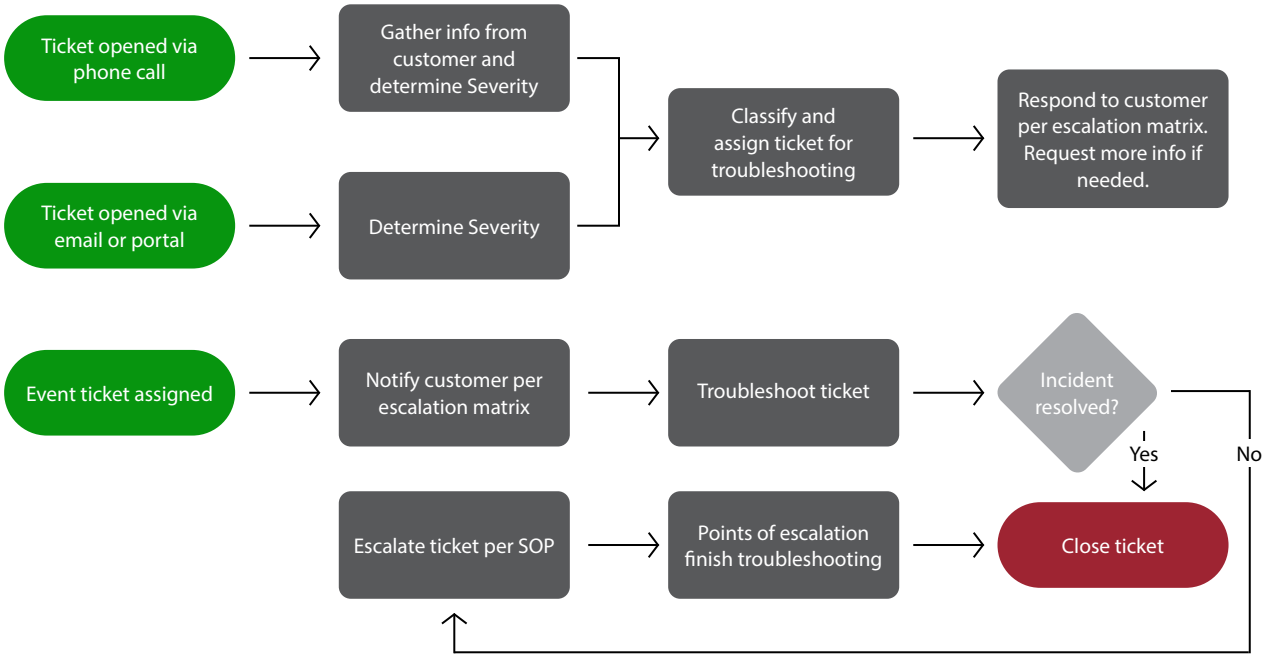
Interface bandwidth utilization

INCIDENT MANAGEMENT

Red River's NOC troubleshoots all incidents logged through Event Management. Additionally, the customer may open incident tickets with Red River's NOC via phone, email, or web portal. When reporting a high priority or critical incident, the customer will open the ticket via phone.

The figure below broadly depicts the overall workflow. Some incidents may be managed by the engineer who first reviews the incidents, while others may be triaged to an engineer with expertise within a specific technology.

FIGURE 4: INCIDENT MANAGEMENT WORKFLOW



ESCALATION AND NOTIFICATION

Upon identifying a new incident, Red River's NOC will notify the customer's approved points of contact. For Sev 1 incidents, a NOC engineer will call escalation contacts in the order defined by the customer until someone is reached on the phone. The NOC engineer will leave a message with each escalation point and will send an email to the defined group as well. Standard escalation methods for each severity level are listed in the table below.

TABLE 1: ESCALATIONS

PRIORITY	PHONE	EMAIL	TICKET UPDATE
P1: Critical	✓	✓	✓
P2: High		✓	✓
P3: Medium			✓
P4: Low			✓

B. Fault Management

The customer may escalate to the NOC for root cause analysis to identify the underlying problem causing a given incident or incidents. Upon identifying the problem, Red River may propose a change to resolve the problem. The customer may approve and assign the change to Red River for completion.

Fault Management tasks include:

- Analyzing one or more related incidents to identify underlying causes
- Logging, categorizing, and diagnosing problems
- Identifying workarounds (if not already identified during incident management)
- Transferring problems into "known errors"
- Identifying solutions to problems
- Proposing changes to resolve problems

Depending upon the impact and cost associated with resolving a problem, the customer may not always elect to have the problem resolved. In such cases, the "known errors" entry will include workarounds to resolve related incidents and will state that permanent resolution of the problem is not currently justified.

C. Patch Management

Red River rolls out patches to our Managed Firewall customer via the Managed Firewall Dashboard.

Red River Patch Management tasks include:

- Scheduled or ad-hoc
- By computer, group, or user-defined collections of computers
- Scans networks for installed and missing security patches
- Automates the tedious process of researching
- Detects vulnerability
- Identifies which patches are installed and date installed
- Determines which patches are needed
- Monitors and maintains patch compliance for entire enterprise

D. Circuits Management

Along with our patch management, Red River will also monitor customer circuits and proactively address any technical issue. This includes contacting the circuit providers to open service tickets.

E. Quarterly Reports

Red River provides customers with access to dashboards and reports where authorized users can view summaries of a wide range of metrics, and can click into the detailed data as needed. The customer's authorized personnel will also have access to Red River's monitoring dashboard, where they can view alerts and logs from configuration items. All users will have access to Red River's ticketing portal to view and open tickets with Red River's Service Desk.

On the following pages are sample dashboards demonstrating common service metrics:

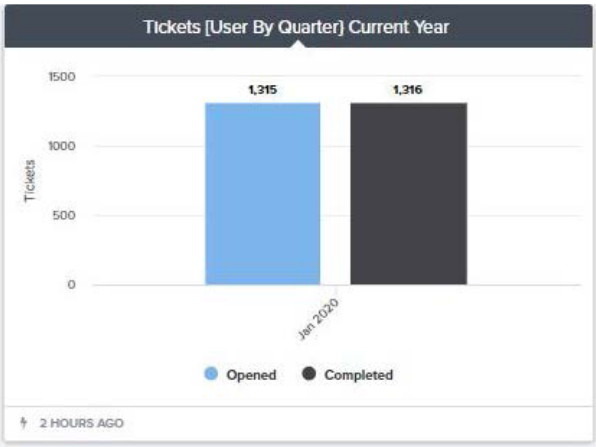
- Customer satisfaction
- Ticket metrics
- SLA performance
- Network performance

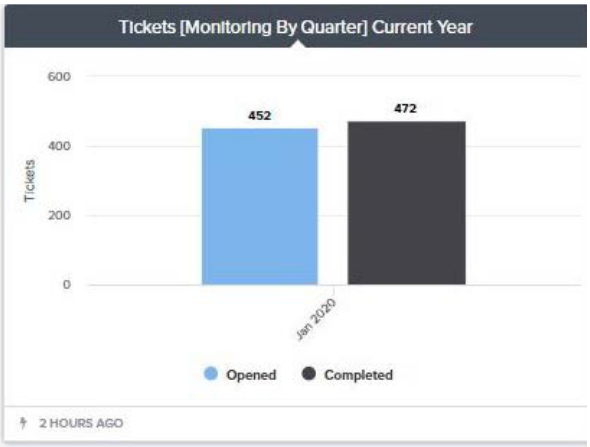
SAMPLE DASHBOARD: CUSTOMER SATISFACTION

Survey [Response By Quarter] Current Year

Month	Sent	Returned	Response
Jan 2020	207	66	31.9%

SAMPLE DASHBOARD: TICKET METRICS

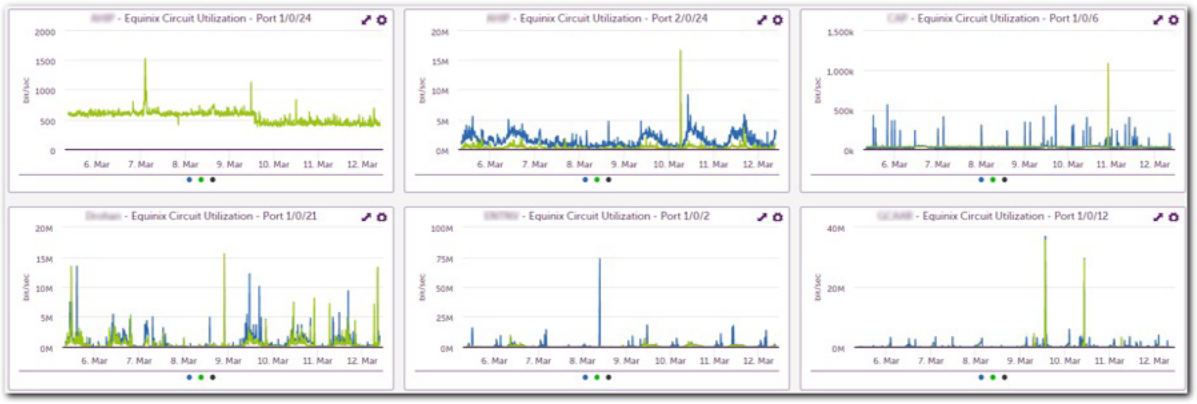




SAMPLE DASHBOARD: SLA PERFORMANCE

Tickets [1st Response] Current Year					
Priority	Total	Met	Miss	No SLA	SLA%
Sev1 Critical	36	35	1	0	97.22%
Sev2 High	24	24	0	0	100.00%
Sev3 Medium	829	829	0	0	100.00%
Sev4 Low/RFC	898	898	0	0	100.00%

NETWORK PERFORMANCE METRICS



PRICING STRUCTURE

Red River will manage the Firewall solution for $150/device/month. This includes 24/7/365 remote support of the Firewall devices as well as carrier circuits from our NOC based in Chantilly, VA.