

Overview

Your organization has made the decision to protect your data assets from malicious intruders. You know that you need to keep these resources secure but you lack the internal experience/resources to know what device/software/solution you need to accomplish your goals. You do not want to hire a dedicated person to handle this...

What's the solution?

CentraSECURE Managed Firewall

CentraComm will work with your team to understand what you want to secure, how you want it protected, and from whom do you want to defend. Once we uncover your goals, we will then implement the policies to ensure that they are met.

Why CentraSECURE Managed Firewall?

Juniper Hardware – CentraComm has standardized on Juniper purpose built firewalls. Juniper's Deep Inspection Firewall's are built on the strength of stateful inspection and integrate intrusion prevention technology into the device to provide application-level attack protection for the network perimeter. Adding deeper protection to the firewall for the types of attacks that threaten small, remote and branch offices and telecommuters with home networks will enable you to stop these threats at the edge and strengthen your overall security stance.

Service Level Commitment – We put our commitments in writing and provide you credits if for any reason we fail to honor those. Our Service Objectives are as follows:

	Response Time	Remedy
Change Request	6 Hours	Credit: 1-Day
Uptime	100% Goal	Credit: 1-Week
Major Network Attack	Notify Within 15 Minutes, Escalation if Necessary	Credit: 1-Week
Hardware Failure	Overnight Replacement with Configuration, 4-Hour Onsite Workaround	Credit: 1-Month
Actual Network Breach	Escalation and Co-operation with 3rd Party Civil or Governmental Agency	Credit: 1-Month

Product Specifications

Managed Hardware & Software—Pro-active monitoring of the hardware and updating of the software to ensure rock-solid reliability and stability

Configuration Management—Installation of initial internal and external security policies, maintenance of backup configuration files for disaster recovery, and an overview of implemented policies.

Monitoring—Monitoring and analysis of ingress and egress traffic flowing through the firewall using Global Pro management software and internal CentraSECURE security framework systems.

Co-management Option— Co-management capability enables you to make changes as needed, with the added assurance that a CentraComm certified engineer will be reviewing all router changes.

Visibility and Reporting— Powerful real-time and historical reporting capabilities to gain insight into usage trends, performance baselines and security events. Use of CentraSECURE web-based monitoring tools for monitoring throughput, performance, and intrusion analysis.

Security Escalation—Escalation of severe or intrusive attacks to 3rd Party Civil and Governmental agencies.

High-Performance Virtual Private Networks—Juniper's award winning hardware-based VPNs for point-to-point and remote access configurations provides high-speed and secure access to remote networks.

Adaptive Security and Countermeasures—When used with Juniper IDP sensors, CentraComm manages a set of policy based actions to be implemented when attacks are recognized.

