Application note

When to safely shut down your firewall

Knowing at which point to sequentially power down your firewall during an outage will help ensure optimal protection for your organization.

There's no downplaying the importance of the firewall appliance within today's network environment. The critical device—considered the first line of defense in network security for more than 25 years—is responsible for monitoring incoming and outgoing network traffic and determining whether to allow or block specific content based on a defined set of security rules.

Modern networks are more vulnerable than ever before, in part due to ever-evolving security vulnerabilities and threat actors seeking new and inventive ways to gain access to a business's network. For instance, malware infections have been on the rise for the last 10 years, according to the 2020 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. Also on the rise are ransomware attacks, phishing schemes and other cybersecurity threats. In addition to more sophisticated hackers, the proliferation of connected devices has opened up new points of entry for cyber criminals.

Firewalls help protect computer networks from unauthorized access, identifying and blocking uninvited content such as worms, viruses and malware. By creating a secure network for multi-person environments, firewalls also help keep private information safe. In addition, they are useful in obstructing specific online sites, beneficial for security purposes and for blocking unsuitable content.

Firewalls are available in different forms, including hardware appliances and software versions that operate on a virtual machine (VM). A hardware model consists of a physical device much like a Linux-based server that resides between the network and gateway. A virtualized firewall, on the other hand, is a piece of software that runs on an operating system that is virtualized. A firewall can also be a piece of software that runs directly on hardware, such as a standard x86 server or appliance.

For applications utilizing hardware appliance-based firewalls, it is important to establish a proper shutdown sequence within your power protection scheme in order to prevent attackers from infiltrating your network and stealing any business information on their network during an outage. An improper shutdown or crash may result in excess downtime.

Complement battery backup with power management tools

Despite the fact that outages create a devastating toll on businesses of all shapes and sizes across every industry, power remains one of the most overlooked aspects of the network. However, a comprehensive power management strategy is vital to safeguard IT equipment including firewalls, keeping critical applications up and running during interruptions. While a reliable uninterruptible power system (UPS) represents the foundation of an effective solution—providing vital battery backup during a power loss—it is just one component. Adding power management software not only enables continuous monitoring of the state of the network environment, batteries and power sources, and the condition of the UPS's internal electronics, it is needed to ensure that connected equipment is properly shut down in the event of an extended outage.

When considering a power management software solution, make sure that it is capable of providing graceful, automatic shutdown of network devices during a prolonged power disruption, which will prevent data loss and save work-in-progress.

Determining the optimal point to shut down your firewall

Using Eaton® Intelligent Power Manager (IPM) software, administrators are able to orchestrate a sequential shutdown of network infrastructure and devices—or even a full infrastructure shutdown— through load shedding, a process where non-critical applications are shut down first in order to extend battery runtime to more essential equipment such as servers. If the battery is at a critical low point, a full infrastructure shutdown will be required.

When operating appliance-based firewalls, administrators may wonder at what point to power down the firewall. Timing is everything. Because the firewall represents the last line of defense, it is important to shut down all other connected equipment first. The firewall should be the final network component that is turned off, just before the management environment itself. Once everything else is powered down, potential points of entry for hackers have been eliminated, giving the firewall nothing further to defend.

Using IPM, this sequential shutdown process can even be deployed in virtual environments to power down VMs and clusters. When IPM detects a power or environmental event, the software orchestrates a graceful shutdown of user VMs and system VMs as required by each individual system or cluster. IPM dynamically executes a preconfigured shutdown policy for system VMs, servers and clusters. Clusters behave differently, but in general, the user VMs should be shut down first.

Consider, for example, a VxRail cluster: IPM begins with a graceful shutdown of system VMs and the VxRail cluster via VxRail Manager API. Once the final host has been shut down, the firewall can then be safely powered down as the last device. Finally, the vSphere (or hypervisor) management environment itself will shut down.

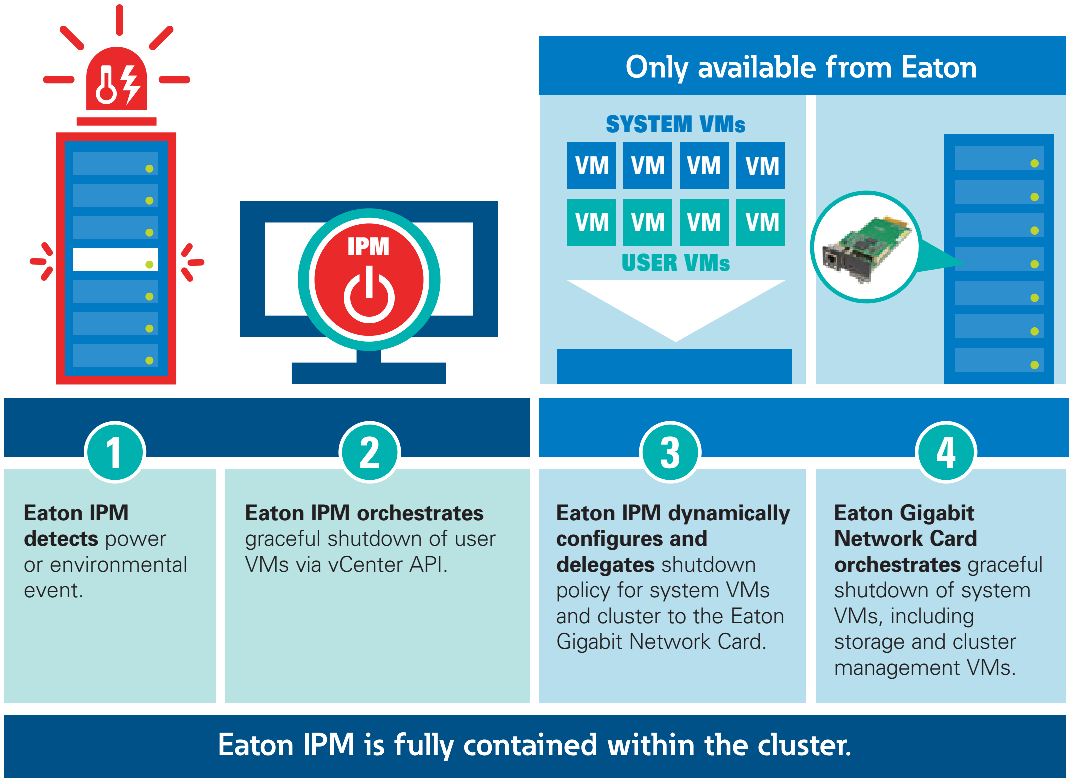
EATON
Powering Business Worldwide

Powering the network back up

Conversely, when electricity is restored and equipment is powered on again, the process should be inverted, with the firewall being the first piece of network equipment to resume operation following the management plane on which vSphere and IPM are running. In this manner, every subsequent device will be safeguarded by the firewall.

The point at which your firewall shuts down during an outage is too important of a consideration to take for granted. The optimal way to ensure that all network devices remain protected is to designate the firewall as the final piece of network equipment to shut down, and the first to resume operation.

√ Data protection solutions within HCI clusters



1. **Eaton IPM detects** power or environmental event.

2. **Eaton IPM orchestrates** graceful shutdown of user VMs via vCenter API.

3. **Eaton IPM dynamically configures and delegates** shutdown policy for system VMs and cluster to the Eaton Gigabit Network Card.

4. **Eaton Gigabit Network Card orchestrates** graceful shutdown of system VMs, including storage and cluster management VMs.

Eaton IPM is fully contained within the cluster.

Learn more about power management solutions
Eaton.com/managesmarter

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP152023EN / GG
March 2021

Follow us on social media to get the
latest product and support information.

Powering Business Worldwide