FIREMON

SOLUTION BRIEF

# Mergers and Acquisitions

*As companies undergo mergers and acquisitions (M&A) activities, they face numerous challenges in ensuring a smooth transition. Whether identifying which network assets to uncouple as part of a divestiture or attempting to integrate disparate systems while maintaining regulatory compliance, without the right tools, teams face an uphill battle. Fortunately, FireMon has multiple solutions that can help address these issues.*

Merging or acquiring another organization's network environment can be a complex and daunting task for any company. It involves combining two different security systems, which likely have been designed and implemented differently, to create a seamless, cohesive, and secure network security infrastructure. Additionally, navigating the intricacies of unraveling assets and networks introduces additional challenges regarding visibility into the network and can potentially introduce risk into this new merged environment.

## M&A Challenges

One of the main challenges faced in this process is acquiring the cyber assets of the other organization. It is not always clear what assets are being acquired, and whether or not they are compliant with industry standards and regulations. This lack of knowledge about the existing assets can lead to potential security risks and vulnerabilities in the merged environment. A lack of understanding of how these assets work together and their place in the network architecture makes it difficult to ensure a smooth integration and may result in misconfigurations or security gaps.

The process of de-threading existing firewall policies also presents major challenges. Detaching the acquired organization's environment from its current setup and integrating it into the acquiring company's infrastructure requires a detailed inventory of assets that need to be removed and identify any overlapping or redundant assets. Moreover, it is crucial to ensure that only the correct assets are removed to prevent any disruptions in network operations.

Unfortunately, most organizations wait until after the merger has been completed to consider their network security management plans, thus causing headaches, errors, and major uplift in the future. Planning this transition prior to the M&A process ensures a smooth and seamless transition for all parties involved.

## M&A Consequences

**Vulnerabilities & Misconfigurations:** Acquiring and merging network security policies introduces the possibility of vulnerabilities and misconfigurations from combining different policies. This increases the risk of cyberattacks, data breaches, financial losses, network disruptions, and damage to the organization's reputation and customer trust.

**Conflicts & Overlap:** Policy conflicts and overlap when merging and acquiring an organization's network policies are also likely, which can create vulnerabilities and weaken the overall security of the network leading to confusion and inconsistencies. Additionally, manual audits by hand are time-consuming and error prone.

**Compliance:** Organizations are subject to various industry-specific regulations and when merging policies, can pose the risk of non-compliance. This can lead to fines and legal issues, impacting an organization's finances, reputation, and customer trust, while also risking network stability and operational efficiency.

**Inefficiency:** Combining policies can introduce redundancies, conflicting rules, and new technologies, causing confusion, delays, and a burden on network security teams, ultimately affecting their productivity and effectiveness.

## Common M&A Mistakes

Improperly planned M&A network activities can create project delays and huge cost overruns, often putting the entire enterprise at risk. As organizations utilize the IT infrastructure to improve business performance, it is incumbent upon them to tackle integration issues upfront to keep costs low and performance high. These efforts include increasing the scope of their M&A due diligence to include a full discovery of both organizations' networks to find overlaps in assets and connectivity.

**Performing a limited IT assessment:** Companies often assume that taking a cross-section of an enterprise network will provide a sufficient model for the entire enterprise.

**Focusing on "getting the deal done":** Organizations often lose sight of how things will look after the first company-to-company connections are made. This lack of comprehensive understanding occurs when the organization limits the scope of IT due diligence to the "as-is" state of the merging companies, instead of the future state envisioned by the merger.

**Failing to understand what the infrastructure actually looks like versus what was envisioned:** Companies often fail to migrate and optimize networks to a converged network from the outset. The result is that within a short time, yet another costly project will be required to clean up legacy systems and connections that still exist in the organization.

## M&A Options

When addressing these challenges organizations have several options to consider:

**Merge everything together and see where the dust settles:** While this may seem like a simple solution, it can result in overlooking important details or potential vulnerabilities.

**Manual audit:** Conducting manual audits for mergers and acquisitions may initially seem cost-effective, but it ultimately entails navigating extensive data, potential errors, time constraints, and intricate system integration, demanding more time and resources than originally envisioned.

**Hiring consultants:** This can provide valuable expertise and guidance in merging and acquiring policies. They can also assist with identifying cyber assets in the environment and reviewing network policies and rules to ensure they align with best practices.

**Leveraging tools:** Tools can detect and identify cyber assets in the network, as well as review policies and rules for any potential conflicts or weaknesses. These tools use advanced algorithms and machine learning to analyze large amounts of data, making it easier for IT teams to identify and address any issues that may arise during the merging and acquiring process.

## FireMon Solutions

FireMon provides a suite of solutions, which include Network Security Policy Management, Cyber Asset Management, and Cloud Security Posture Management, helping enable companies to smoothly navigate M&A activities by ensuring a secure transition through the comprehensive management and security of their network policies. These tools collaborate seamlessly to offer a holistic approach for safeguarding and managing the network throughout the merger or acquisition.

### Network Security Policy Management

FireMon Policy Manager helps organizations identify and address conflicting policies and rules during network mergers, ensuring network security integrity through ongoing monitoring and vulnerability/compliance issue detection.

- Centralized management of network security policies and rules
- Automated policy change tracking and impact analysis
- Continuous compliance assessment against industry regulations and best practices
- Integration with popular firewall vendors for seamless policy management

### Cyber Asset Management

FireMon Asset Manager aids organizations in identifying and assessing all assets within the merged network, including hardware and software, enabling informed decisions regarding asset retention or retirement by providing insights into vulnerabilities and potential risks.

- Automatic discovery of all network devices and applications
- Real-time asset tracking and monitoring
- Integration with vulnerability management tools
- Customizable asset groupings and classifications for easier management
- Even in the best run networks, Asset Manager has found that administrators are unaware of as much as 20% of their actual network assets.

### Cloud Security Posture Management

In today's corporate landscape, integrating cloud services into networks during mergers and acquisitions is commonplace, and FireMon Cloud Defense assists organizations by evaluating and verifying the security compliance of potential new cloud services before their integration.

- Automated discovery and assessment of new cloud services
- Continuous compliance monitoring and reporting
- Integration with popular cloud service providers for seamless management and security control

## Why FireMon?

Unlike the alternative options, FireMon offers comprehensive solutions that help organizations overcome challenges in the pre- and post-M&A stages. FireMon's scalable, flexible, and customizable solutions meet the needs and challenges of organizations across the globe.

### Achieve and Maintain Compliance

After completing an M&A, maintaining compliance can be a challenge due to the differences in regulatory requirements. FireMon ensures organizations achieve and maintain compliance with real-network and device discovery, comprehensive asset identification, and out-of-the-box compliance reporting.

### Reduce Risk

M&A can pose a significant risk to an organization's security, given that both companies may have different security policies, systems, and protocols. This can create vulnerabilities that cybercriminals can exploit. FireMon provides comprehensive security solutions that help organizations understand their security posture, identify potential risk areas, and implement security controls.

### Improve Operational Efficiency

FireMon helps organizations manage and integrate their network security operations. With a single pane of glass view, IT teams see all network security policies across the organization, enabling a centralized management plan and granular visibility into all firewalls.

With a robust approach to cyber asset management, network security policy management, and cloud security posture assessment, organizations can effectively navigate through the complexities of merging networks while maintaining a high level of security and compliance with FireMon.

**For more information about how FireMon can help you perform IT due diligence for M&A activities, please email: sales@firemon.com**

## Case Study:

Fortune 500 Corporation Identifies Active Divested Company Connections in Enterprise Network

### Business Challenge:

One of the largest oilfield services companies was implementing a major divestiture of their construction and project management subsidiary. The client's major focus was to prevent any business disruptions that could occur from the network segmentation of the main company and the spinoff division. The combined network is over 300,000 IP addresses and many business processes are run across the combined networks.

### Solution:

FireMon ran an initial Asset Manager Network Assessment service over a 90-day time frame. With the use of interactive mapping and visualization, a complete and thorough understanding of this interconnectivity and touch points was easily uncovered.

### Results:

This visualization and database results included:

- Routers with shared interfaces; interfaces still up and running
- Multiple ingress/egress points into both enterprises
- Leak paths uncovered while verifying the divestiture
- Multiple devices identified with residual community strings
- Multiple Internet connections
- Shared network addressing schemes needing remediation

The results provided a clear roadmap for the client in its effort to become completely divested of its subsidiary.

FIREMON

FireMon's mission is to improve security operations that will in turn lead to better security outcomes. FireMon delivers industry-leading security policy management, cloud security operations, and asset management solutions to over 1,700 enterprises in nearly 70 countries. Our security policy management platform is the only real-time solution that reduces firewall and cloud security policy-related risks, manages policy changes, and enforces compliance. FireMon's Cloud Defense (formerly DisruptOps) offering is the only distributed cloud security operations offering that detects and responds to issues in the fast-paced public cloud environments such as AWS and Azure. Our cloud-based Asset Management solution (formerly Lumeta) can scan an entire enterprise infrastructure, from on-premises networks to the cloud, to identify everything in the environment and provide valuable insights into how it's all connected together. Learn more at FireMon.com and the FireMon Blog.