Five Critical Rules for Firewall Management:

Lessons from the Field

Executive Summary

Firewall management remains an organisation's primary network defence. It commands more time from network security managers than virtually any other activity. And it's easy to get wrong, particularly by IT administrators doing double duty as their organisations' IT security staff.

Dell SecureWorks' network security team identified five focus areas for IT managers when managing their firewall. Our security engineers provide real-life cases to highlight the importance of these recommendations. The actions outlined below can help IT managers save time, money and administrative burden.

We advise administrators to consider the following suggestions for more effective firewall management:

- **Clearly define your change management plan.** Centralised firewall management authority and a documented process can help prevent unwanted changes to the current configuration of the network, limiting the chance that a change will impair functionality, hinder future changes or open a hole in network security.
- **Test major firewall changes before going live.** Make sure to test major firewall changes before they are implemented in production. If possible, build a testing environment that mirrors production systems. Failure to adequately test changes could lead to business disruption such as network latency issues or complete network outages.
- **Protect yourself by taking a configuration snapshot before making major changes to your firewall.** It's crucial to have a change reversion system in place, with failover and recovery plans, before an urgent need emerges. Consistent system snapshots can save time and money if a migration goes wrong or equipment fails unexpectedly.
- **Monitor user access to the firewall configuration.** User access logs can act as an elementary intrusion detection system, potentially revealing unauthorised access attempts from within or outside the network. Logs can also reveal creeping, incremental and unwanted changes to security policy.
- **Schedule regular policy audits.** Over time, rules may not match security policy and unused rules may clog traffic and present a barrier to network changes. Out-of-step security can also present legal risks. It's important to regularly review your firewall policy, update it as needed, and then check adherence to that policy by reviewing the firewall rules and configuration.

Clearly define your change management plan

You shouldn't fear change to your firewall rules. It's a natural and necessary component of a growing company and can reflect shifts in the security environment or evolving needs among the user base. But without a clearly understood change management plan even a seemingly simple rule change on a firewall can create a disastrous ripple effect across an organisation's network.

Change management plans mitigate risk. An effective change management plan captures important metrics during alterations to access rules. These metrics–for example, a precipitous drop-off in IP traffic or a dramatic increase from a particular domain–can identify weaknesses or failures during the change. This kind of monitoring can provide an early warning of widespread outages or a significant impact to critical systems and service levels. It also provides an audit record to measure the success or failure of a series of changes over time, for comparison.

A change management plan should:

- Establish an accepted approach for requesting policy changes and setting policy requirements
- Implement proper controls, identifying who can and cannot authorise a change
- Centralise firewall management to efficiently create, distribute and enforce policies
- Describe the required communication and coordination points for properly processing any changes
- Create an audit trail to track requests, actions and results of a firewall change

Change management requires more than a set of software tools. It is a process that enforces discipline on the network and requires agreement from everyone with access to the firewall configuration. Without clear communication about policy and priorities, a change management system will eventually be undermined by the behaviour of network clients.

Test major firewall changes before going live

Modifying a firewall introduces business risk. The more damage a serious disruption might create, the greater the value of testing a configuration before going live.

It is prudent to avoid editing firewall rules on the production device guarding your systems. One possible solution is to test changes in a virtual sandbox mirroring your systems, running as a lab environment. These machines should be separate from your live systems, either physically or through an incomplete network interface configuration.

If it isn't practical to maintain a testing environment, policy changes can be implemented on a central management console and pushed as a policy update to the firewall. Doing so allows for easier reversion than a physical swap, which should include much more serious testing before going live.

Allow ample time to execute a solid test before making a significant change to firewall configurations.

Firewall change testing plans should:

- Review security policies of all the machines on the network for consistency as well as failover and recovery plans
- Ensure that the firewall itself has adequate access security
- Perform a test on both inbound and outbound data using an appropriate packet sniffer
- Confirm that the firewall is allowing and blocking data according to the established policies and rule sets
- Complete a performance test to determine how a new configuration enhances or degrades network activity, particularly for VPNs
- Check the compatibility and interoperability of the firewall with other applications and equipment on the network – particularly from heterogeneous vendors and sources
- Create an audit trail for trend and root-cause analysis

A good point to mention is that we see far too many companies using end-of-life firewall systems that contain limited patch management capabilities. A patch management system can help administer changes consistently throughout the network on a known schedule, without leaving individual systems unmodified or allowing multiple simultaneous modifications to a firewall. A patch management system can also prevent unwanted changes to the current configuration of the network, limiting the chance that a change will impair functionality.

Protect yourself by taking a configuration snapshot before making changes to your firewall

The worst problems with a configuration change tend to happen while other problems emerge, turning a challenge into a catastrophe. Imagine a customer-facing, revenue-generating website under a distributed denial of service (DDoS) attack, requiring significant firewall configuration changes to thwart. Under these circumstances, there's often no time to test. For this and similar reasons, it's vital to have a change reversion system in place with failover and recovery plans, before the urgent need emerges.

Though configuration snapshots are often an afterthought – except during a significant problem – they are a vital part of a change reversion system. Many platforms can take snapshots. Check Point Software's SecurePlatform Image and configuration can be saved and reverted with the revert command and the snapshot utility. Juniper, IBM and other providers also have systems with snapshot capabilities.

Over time, these snapshots can do more than provide for a safe transition to a new configuration – they can build a profile of network activity. This profiling can help monitor a network's feature usage as well as detect anomalous behaviour, over-subscription and load issues.

Configuration snapshot tools may be set up to send a report automatically, on a daily basis. As changes occur, the report permits IT managers to look back at previous configurations. It also allows administrators to clone a machine if a device simply fails without warning.

A few tips for managing a configuration change:

- When migrating to a new firewall, harden the firewall system to protect the network against unauthorised access. The configuration process can present a temporary security vulnerability. Install patches and console software needed for remote access at this time. Only the administrator doing that work should be able to manage the firewall during the configuration. All other management services for the firewall should be disabled. Create subordinate administrator accounts only after the network has been properly configured.
- Synchronise the internal clocks for each firewall with all of your other network equipment to make sure logs can be compared accurately.
- Don't keep the backup firewall configuration files on your network! If your network crashes, you won't have access to them.

We've seen too many companies have to completely rebuild their firewalls from scratch after a failure. While it may seem obvious, maintaining current backups is vital to any solid security programme.

Monitor user access to firewall configuration

Scrupulous IT security administrators watch their firewall traffic. Barring a gaping hole in your network security, the firewall is a single point of entry to the network and contains evidence of unwanted connections. The firewall can reveal malicious code, Trojan horses and root kits through alerts of denied connections or too many connections permitted.

Reading a firewall traffic log can be somewhat confusing, but user access logs tend to be much simpler and can act as a basic intrusion detection system. User logs provide two very important kinds of security data. First, the logs can track policy creep. If administrators with firewall configuration change access login and make unauthorised alterations to the firewall, it could compromise the overall adherence to security requirements and cause instability during migrations.

Second, the log may reveal unauthorised access attempts from within or outside the network. Unsuccessful logins to your firewall or to other mission-critical servers could be a sign of a penetration attempt, and may prompt you to block or drop all connections from that domain or IP address as a rule. If you plan to create such a rule, check whether the IP address has been spoofed.

Similarly, unexpected outbound connections may be a sign that an unauthorised user has gained access to your system and is using it as a launching pad for spam or to attack other computers from your Web server.

We recommend that you review the access list regularly – perhaps as often as once a day – to see if anyone has made changes to the firewall rules. IT managers should maintain a named list of people with authorisation to make firewall rule changes, and that list should be kept secure... offline. Maintaining this list should be part of an overall change management plan, so people with administrative access understand how to make rule changes properly. Most major firewall platform products provide user access logs.

Of course, the log itself has to be secure, or else a serious intruder could alter the content to eliminate evidence of a penetration. If you can, create one or more administrative user accounts with read-only access to the logs and use these credentials to audit logs.

Schedule regular policy audits

Firewall security means nothing without a coherent security policy – the combination of rules and principles around which your security has been built. Your firewall enforces your security policy, but it doesn't create it. You do.

Unfortunately, firewall security policy is often a "set and forget" matter that evolves ad hoc from short-term rule changes and not from the changing needs of the organisation or the changing security environment. Over time, rules may not match security policy, and unused rules may clog traffic and hinder change.

Out-of-step security can also present legal risk, given frequent changes in data security regulatory requirements for processing credit card data, managing securities compliance, holding medical and financial information, and others.

Firewall data should be collected and evaluated on a regular schedule, with the goal of harmonising access rules with the overall security posture, to uncover policy violations and other issues. The timing of this review should be proportionate to the frequency of firewall rule changes, listing the changes made since the last regular review, who made those changes and why those changes were made.

Suggested times to review policy are when you:

- Introduce new firewall or other security that significantly alters your network capabilities
- Introduce new IP-capable applications to the network
- Change to a new ISP (Internet Service Provider)
- Begin sharing network traffic in collaboration with a business partner
- Undergo a significant business or operational change
- Sustain significant personnel turnover

Good network security operates in layers that work together to protect assets. Any firewall policy review should ensure that firewall layers operate in the right order, with the firewall set to accept the most traffic when positioned closest to the outside and firewalls accepting the least traffic closest to the data to be protected. Enable port filtering at the outer edge of the network and content filtering as close to the content receiver as possible. This approach creates zones of security.

Conclusion

As a first line of network defence, firewalls are critical to protect IT assets from compromise and disruption. Changing business and security demands make proper firewall management a challenge for many organisations, especially those constrained by limited security resources and staff.

The recommendations in this paper by no means provide a comprehensive list of the tasks that are required to keep a firewall functioning effectively, but they are important components of any sound firewall management programme. Following the five guidelines will help you avoid the negative scenarios illustrated in the cases and, as a result, get better protection from your network firewalls and reduce risk to your organisation.

About Dell SecureWorks

Should you have any questions about how Dell SecureWorks can help your organisation manage firewalls with greater efficiency and effectiveness, contact your account manager, email info@secureworks.com or call (877) 905-6661.

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognised as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organisations of all sizes protect their IT assets, comply with regulations and reduce security costs.

For more information, visit http://www.secureworks.com/uk