Five Critical Rules for Firewall Management: Lessons from the Field
Executive Summary

Firewall management remains an organization’s primary network defense. 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 organizations’ 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.** Centralized 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 unauthorized 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 organization’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 authorize a change
- Centralize 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 behavior of network clients.

Case #1 – A change gone wrong.

“I used to manage the firewalls at a large pension management firm. One of our IT executives was a Certified Information Systems Security Professional, but didn’t have a whole lot of practical sense.

One day, I was in our Network Operations Center (NOC) and I happened to pick up the phone when he called in. “The firewall is not blocking pop-ups.” Ok, that’s true. The firewall did antivirus and some intrusion detection stuff, but it was never a built-in pop-up blocker. “I want it to block pop-ups,” he ranted.

“Uh, sir… the firewall wasn’t designed to block pop-ups. The only way I can get this done is by blocking port 80 outbound. This is certain to upset your users,” I cautioned.

He cut me off before I could explain. “Just do it.”

I tried again with no luck changing his mind. Then I asked for a written request, signed and encrypted with his PGP key, so that there would be no chance of repudiation. Two minutes later, he submitted the change request as an emergency order, which meant to do it within an hour. I made the change. We waited.

Five minutes passed. My boss jacked into my phone, muted, to back me up for following the procedures as I was ordered, even though I advised against it. The IT executive called back into the NOC.

“THE INTERNET ISN’T WORKING!?”

I sent him to a site that I knew would let him use HTTPS on the first page. He could get there. “Well, then, the Internet is working,” I said.

In apoplexy, he shouted, “WE CAN’T BROWSE REGULAR WEB PAGES!”

“Um, that’s correct,” I said. “You told me to block that.”

“CHANGE IT BACK NOW!”

My boss and I waited patiently for the call I knew was coming in. The chief information officer called a moment later. I explained what happened, and why I had to follow procedure, but since he was involved now I could go ahead and change everything back. He ended the call with, “And please take him off of the authorization list.”
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.

---

Case #2 – Upgrade live.

“I was a new-hire network engineer at a small manufacturing firm and was asked to upgrade our firewalls to a fairly new version of software. I had previously had numerous problems with upgrading to this version, so bad that it took hours to recover, due to a number of bugs and poor implementation on the vendor’s part. Knowing this, I warned the senior manager that upgrading to that version should not be done unless it was absolutely necessary, and that it would not be a quick process. We found out that the current version of software our firewalls used would support the functions we were looking to implement. This had not been formally documented in the release notes for the version of software we were running; however, the vendor did provide written documentation stating it would work. Despite this, our managers still insisted on proceeding with the upgrade.

The next morning we began upgrading the firewalls. Upon rebooting the first one to the new version of software, we immediately ran into problems. The upgrade scripts the vendor had implemented did not work, we encountered numerous bugs, and the firewall was stuck in a constant loop that allowed for no commands to be executed on it.

We had to reboot the firewall numerous times and go into a special mode to recover the device and bring it back to the previous working version of software. The entire process took out the network for several hours and could have been easily avoided with sufficient testing.”
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. Cisco ASA 5500 Series Adaptive Security Appliances have snapshot capability and can email configuration snapshots to a system administrator. 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 behavior, 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 unauthorized 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.

- Synchronize 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 snapshots is vital to any solid security program.

Case #3 – How was that configured?

"An online gaming company contacted a security firm, not to build a security system, but to rebuild it. The gaming company measured its losses in dollars per minute when user access merely slows down, much less stopped entirely. And, earlier, some network problem had slowed access, meaning players couldn’t reach the virtual tables.

In this case, the company wasn’t under attack, but it looked like it at first. Customers had been denied service for hours and executives believed some would migrate to competitors. Terrified, they began to change out anything they thought might be part of the problem—switches, routers, load balancers…and firewall configurations.

A day later, they discovered that part of the problem was on a RAID disk that had gone down, slowing service as it was rebuilt. They found a second problem later—a virus that had exacerbated the slowdown.

But the most significant problem at that point was their reaction to the first problem. The company’s zeal to switch out all of their equipment had left them without any idea at all about their original, successful configuration. No one had documented the original configuration, or any of the changes.

It took the company several days to return to full operational strength, at a total cost of millions in lost business."
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 unauthorized alterations to the firewall, it could compromise the overall adherence to security requirements and cause instability during migrations.

Second, the log may reveal unauthorized 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 unauthorized 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 authorization 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.

Case #4 – Who goes there? Blood Elves, apparently.

“A midsize technology firm audited their network and discovered a cabal of World of Warcraft (WoW) players had installed the game on their laptops—which was permitted—and were playing the game at work—which was not.

After much debate, rather than force an uninstall of the client, they decided to ban the game at work and block the WoW ports at the company firewall.

A few weeks went by and network traffic had dipped. Suddenly, they found the network had slowed way down again. Confused, the network administrator looked through the firewall access logs and discovered that someone had been opening and closing the WoW ports using a dummy account.

The IT manager wanted to know who had subverted system security, so he left things in place for a while. Not long after, by carefully watching the logs, he found one of the graphic design interns was responsible for the security breach. He had stolen the main firewall password to create the dummy account. Apparently, he had a serious addiction to the game, logging 60 to 70 hours of play a week, including most of his time at work. The intern was dismissed.

Another few weeks went by and the company started seeing strange traffic again. This time, it seemingly had nothing to do with WoW. The traffic was originating at port 1080, so, at first, they thought the traffic was from Skype which they used for video teleconferences and international phone calls. IT considered upgrading bandwidth, but the logs didn’t really match the Internet traffic patterns.

After more monitoring, they found an answer. Two other employees had downloaded PuTTY, a free implementation of Telnet and SSH for Windows and Unix platforms. PuTTY allows users to connect to a virtual PC using a tunnel through the firewall. PuTTY also uses port 1080. The pair had been connecting from work to their home computers and from there to the WoW game servers. Like the intern, these two employees were also fired.”
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 organization 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 harmonizing 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.

Case #5 – Know your policy.

“I once worked for a company that was going through a merger with a midsize competitor. It’s easy enough to say that mergers can be a difficult IT challenge. This one seemed worse than most.

To start, other than the fact that we both ran on Microsoft platforms, we used no common software or hardware.

But the equipment wasn’t the real problem. We had a culture problem, and it had a direct effect on implementing a consistent security policy across the network. While the executives and sales staff meshed well culturally, the IT staff came from very different backgrounds and held very different security philosophies. Their side of the firm had been recruited largely from network service providers and preferred to work with home-brewed network systems, warts and all. Meanwhile, our side of the firm had generally relied on close collaboration with partners and vendors for technical support and security advice.

The problems began to emerge as we started to set our network security policies. Our IT chief had taken over the department and wanted a relatively uniform access management policy. Over the next year as we started to implement the policy, it became clear that some IT staff were liberally implementing short-term exceptions, case-by-case, that somehow grew into long-term exceptions. Our department was focused on integrating our customer relationship management systems and our databases for the public-facing site, so security issues slipped into the background.

Meanwhile, we were losing staff after the merger, mostly from the other team as they went looking for a less frenetic environment.

About a year after the merger, a data thief penetrated our network and stole some customer data. The data itself wasn’t particularly damaging—names and phone numbers, no social security numbers or credit card information—but the event was significant for us. We instantly focused on security.

The CIO started a security policy review and discovered that half of our network was a patchwork mess of contradictory rule sets, which had contributed to the breach. It took a staff of five people three weeks of change management and testing to resolve the security problems.”
Conclusion

As a first line of network defense, firewalls are critical to protect IT assets from compromise and disruption. Changing business and security demands make proper firewall management a challenge for many organizations, 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 program. 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 organization.

About Dell SecureWorks

Should you have any questions about how Dell SecureWorks can help your organization 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. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.