Tufin conducted its annual firewall management insight survey amongst 200 network security professionals. The study found that 93.6 percent of all firewall change requests are application-related, validating that the function of firewalls has evolved to include secure application connectivity, in addition to their traditional role of perimeter security.

- Almost half of respondents audit their firewalls only once a year and 15% never audit their firewalls; 50% spend up to a week or more per quarter on firewall audits.
- Almost 1/5 reported they knew of someone who cheated on an audit because they either felt the audit was a waste of time (39.3%) or they did not have enough time/resources (35.6%).
- Almost 1/5 of the sample has no idea how current their firewall policy is.
- 40% have no way to know when a rule needs to be expired or recertified.
- 30% never test configuration changes before they are implemented.
- 90% of the sample has to redo up to half of all network security changes because they do not meet design requirements.

While survey data indicates firewalls are becoming increasingly relevant outside of their established function in security operations, their role have expanded - not shifted. Firewall management processes can have a significant impact on an organization’s risk posture.
Q. What is the most common cause for a firewall change request?

- New employee: 4.0%
- New application: 6.9%
- Change to an existing application: 12.1%
- Migrating/moving servers to different location: 27.2%
- Decommissioning: 47.4%
- Removing access: 2.3%

Q. What percentage of network security changes implemented need to be modified because the design does not meet the requirements?

- Less than 25%: 50.6%
- Between 25-50%: 39.8%
- More than 50%: 9.7%
Q. How long does it take from the time a change request is submitted until it’s completed (in production)?

- 33.3% Same day
- 12.7% Within 1 day
- 35.4% 2-3 days
- 13.2% 1-2 weeks
- 5.4% More than 2 weeks

Q. How often does a firewall change need to be redone?

- 58.5% 0-20% of the time
- 23.9% 20-40% of the time
- 14.8% 40-60% of the time
- 0.6% 61-80% of the time
- 2.3% 81-100% of the time
Q. Why do firewall changes need to be redone?

- Change was based on inaccurate data (43.4%)
- New rule conflicted with another one (17.7%)
- There was a typo in one of the fields – human error (13.7%)
- Miscommunication between the firewall team and the person that requested the change (25.1%)

Q. How do you know when a firewall configuration change causes downtime?

- Increased communications reporting the issue (53.7%)
- Automated system alerts us to the problem (43.4%)
- An alternative method (2.9%)
Q. Do you think your current change management processes put you at risk of a security breach?

- Yes: 31.7%
- No: 38.6%
- Not sure: 29.6%

Q. What percentage of your rule base is obsolete (unused, or no longer required)?

- Less than 5%: 18.5%
- Less than 25%: 7.4%
- Less than 50%: 37.6%
- Over 50%: 16.9%
- I don't know: 19.6%
Q. How do you know when a firewall rule needs to be recertified or decommissioned?

- 40.0%: Quarterly or annual audit
- 30.0%: We don’t
- 23.2%: Automated firewall management system flags it
- 6.8%: Word/Excel document

Q. How do you tighten overly permissive firewall rules?

- 47.1%: We use an automated solution
- 30.5%: Manually, by inspecting log information
- 22.5%: We don’t tighten rules because it takes too long
- 6.8%: Word/Excel document
Q. Have you, or any of your colleagues, ever been asked to make a rule/configuration change against your better judgment?

- 58.0% Yes
- 23.9% No
- 18.2% I don’t know

Q. What percentage of your organization’s total firewall changes are application-related?

- 46.8% Less than 50%
- 32.3% Between 50-80%
- 21.0% Between 80-100%
Q. How does your organization keep track of application connectivity requirements?

- 18.1% Excel or Word document
- 41.2% Comments in the firewall rule base
- 27.1% A home-grown system
- 13.6% We don’t

Q. Are you confident that as a team, you only open the ports required by your business?

- 46.3% Yes
- 29.7% No
- 24.0% Not sure
Q. Has your organization had a security breach due to an application-related rule change?

- 30.1% Yes
- 53.2% No
- 16.8% Not sure

Q. How often has your organization experienced application service disruptions due to network configuration changes?

- 51.1% More than 20 times/year
- 19.0% Between 10 and 20 times/year
- 20.7% Less than 10 times/year
- 9.2% Not sure
Q. How frequently do you perform corporate and/or regulatory audits?

- 45.2% Every month
- 20.4% Every quarter
- 13.4% Every six months
- 13.4% Every year
- 7.5% Never
- 2.1% Less than a day per quarter – it’s automated
- 1.6% We don’t do audits
- 1.6% 1-2 days/quarter
- 1.6% 3-7 days/quarter
- 1.6% Over 7 days/quarter

Q. How much time does the network security team spend on firewall audits, both in preparation and in the audit itself?

- 31.1% Over 7 days/quarter
- 22.4% 3-7 days/quarter
- 20.8% 1-2 days/quarter
- 15.8% Less than a day per quarter – it’s automated
- 9.8% We don’t do audits
Q. Do you know anyone who ever cheated on an audit?

- Yes: 18.8%
- No: 81.3%

Q. If you answered “Yes” to the previous question, please explain why

- Not enough time / resources: 15.3%
- The areas they were auditing were irrelevant to the business: 39.0%
- The audit was a waste of time: 35.6%
- Worried about themselves or someone else looking bad: 10.2%
Q. What percentage of your security budget is spent on items that don’t improve security?

- A huge amount: 34.3%
- Quite a lot: 22.9%
- A little: 22.9%
- Not much: 12.6%
- I don’t know: 7.4%

Q. Do you test or simulate configuration changes for potential risk and compliance violations before you implement them in production?

- All the time: 30.6%
- Most of the time: 27.4%
- For critical changes only: 25.3%
- Never: 16.7%
Conclusions

This report reveals that the role firewalls play in managing application connectivity is both a cause and effect of sweeping trends in enterprise IT. It is clear that more needs to be done in terms of education and understanding of the advantages that firewall security automation brings to the business efficiency table and how it allows the right set of organizational processes between the relevant stakeholders to be defined and implemented.

Learn more about how Tufin has addressed these enterprise IT trends from the 2012 launch of SecureApp, to the new release of Tufin Security Suite (TSS), its award winning Security Policy Management solution.

Read the SIX Group case study to learn how – with SecureApp – they can now report dramatic improvements in application connectivity-related change management processes.

Join the discussion about this report, or any other security policy management issues.

Your Opinion Matters
Twitter: http://twitter.com/TufinTech
Facebook: http://www.facebook.com/Tufintech
Google+: https://plus.google.com/s/tufin
LinkedIn: http://www.linkedin.com/companies/tufin-technologies
YouTube: http://www.youtube.com/user/Tufintech
The Tufin Blog: http://www.tufin.com/blog

About Tufin Technologies
Tufin™ is the leading provider of Security Policy Management solutions that enable companies to cost-effectively manage their firewall, switch and router policies, reduce security and business continuity risks, and ensure Continuous Compliance with regulatory standards. The award-winning Tufin Security Suite provides security teams with powerful automation that slashes the time and costs spent managing change and successfully passing audits. Founded in 2005, Tufin serves more than 1,100 customers in industries from telecom and financial services to energy, transportation and pharmaceuticals. Tufin partners with leading vendors including Check Point, Cisco, Juniper Networks, Palo Alto Networks, Fortinet, F5, Blue Coat, McAfee and BMC Software, and is known for technological innovation and dedicated customer service.