tufin The Security Policy Company.

Top 5 Network Operations Pain Points and How to Overcome Them.

Network changes that meet dynamic business requirements, such as adding new servers, updating firewall rules and decommissioning objects, can be arduous. That's because they're requested more frequently, and when done manually, they become the main pain point of every network and server admin we've talked to. It's also a tough balancing act. When it takes too long to implement a change, it can likely delay the launch of a new service. However, if you implement a change too quickly, without first checking its impact on your network, it can result in configuration errors, exposing your network to potential risks.

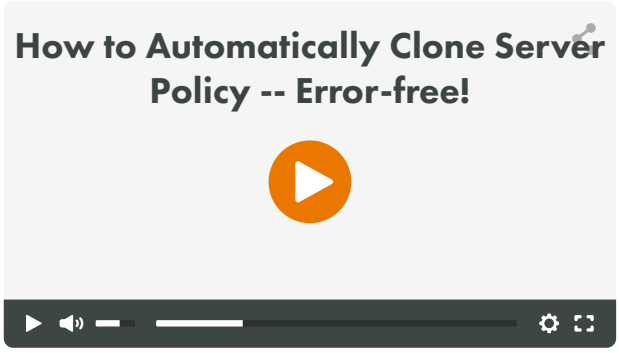
Here are five of the most common challenges when dealing with network-related changes. How many do you identify with?

1 Server cloning

Server admins constantly ask network and firewall admins to add firewall rules for new servers. These requests typically come in as, "Can you please grant server Y, which is a new server, the same network access as server X?"

For most server admins, this is where their involvement usually stops. From their perspective, they've done their part—the server is online and ready to go. But this is actually where the network/firewall teams' battle begins.

Often the case is that no one knows what server X has access to, specifically which areas of the network, and which security zones it can traverse. This is where Tufin can help. Server cloning, using **Tufin SecureChange**, will locate all relevant access rules across your entire environment, and automatically add the new server Y to these rules. No more long hours or even days of tracking down the particulars - firewall by firewall, rule by rule, and object by object - to add a new server to the mix.



Watch this short video (2 min.) (https://tinyurl.com/y6xas8kx) to learn how you can automatically replace old/add a new server – to save time and eliminate the risk of misconfigurations with Tufin SecureChange.

2 Server decommissioning

Given the above scenario, when server admins are adding the new server Y to the network, is it to replace another server (server X) that's out-of-date and soon to be shut down?

If that's the case, how can you ensure you removed server X's access to the network? Do you have to crawl the firewalls one by one, or do you (hopefully) have a searchable index of rules somewhere?

The server decommission workflow is Tufin's answer to removing access to servers that are no longer needed on the network. By doing this, you reduce the risk of that server's old IP address is reassigned and used, for example, by malicious users to access other assets.

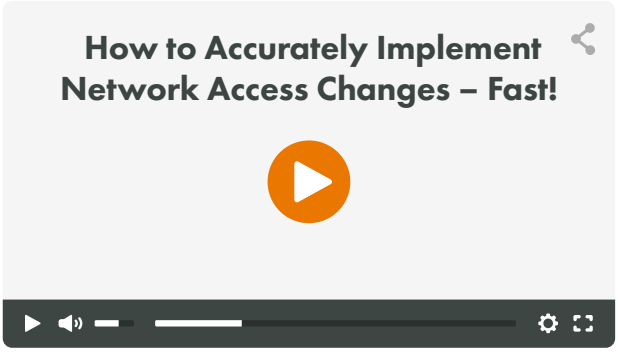
Tufin can also integrate with your ITSM so when the server folks update the server records, assuming it's been decommissioned, it will automatically trigger an API call to Tufin SecureChange and create a server decommission ticket. This way, Tufin manages the task of removing the old server's access while you retain control over the process.

Watch this short video (2.5 min.) (https://tinyurl.com/y6dv8275) **to learn how you can automatically decommission a server – from impact assessment to risk-free removal with Tufin SecureChange.**

3 Apps connectivity requests

Firewall administrators are constantly working tickets with some organizations have been tackling over 1,000 changes per month for routine firewall requests. Engineers, who have numerous other tasks, such as upgrading firewalls, upgrading/replacing aging network infrastructure, and troubleshooting common network issues, often handle these changes manually, which results in significant operational overhead and delays in implementing changes. Tufin SecureChange provides a workflow that can help you expedite the process and even handle it for you.

Tufin can integrate with your existing ticketing system or even act as your management console for ticket handling. Once Tufin is on board, you can fully automate the workflow that will identify where the rules should be implemented, ensure they're not already implemented, check them against your defined security policy, and even push out the change as scheduled.



Watch this short video (4.0 min.) (https://tinyurl.com/y3nxpvmx) **to learn how you can implement network access changes quickly and accurately with Tufin SecureChange.**

4 Rule recertification

How many times have firewall/security teams been asked the question, "Can you please open X, Y and Z ports to servers A, B and C for 90 days, while we test a new widget?"

This happens repeatedly involving multiple teams who are constantly trying out new technology that requires access to other areas of the network, and even the internet. But, with understaffed network/security teams who are always on the go, who remembers 91 days from now to remove that rule?

With Tufin, you can easily see upcoming rules that are set to expire, and with a few simple clicks, the designated admin can extend the time needed or confirm that rules can be disabled or removed.

Watch this short video (3 min.) (https://tinyurl.com/y6dv8275) **to learn how using the Tufin SecureChange built-in workflow you can automatically manage rule certification process.**

5 Vulnerability-free server deployment

When a server admin deploys a new server and requests it to be granted access, typically, the new server is added manually to all firewalls in the environment.

But, has the server OS been patched? Has it been updated to its latest OS version?

Does it have a critical vulnerability that should prevent it from being exposed to the network? How do you know? And when do you find out, if you find out at all?

Tufin can help answer these questions with API integration into your existing vulnerability scanner. By integrating Tufin SecureChange with your scanner, you can automatically check to see if the server has been scanned, and if not, Tufin can request a scan. It's recommended that you add this task to the process, so before your network team grants approval, a check can be added to verify the server's network readiness.

These are just five examples of how the Tufin Orchestration Suite can accelerate and simplify security management and operations. When all is said and done, you'll have improved the accuracy of the changes made, and take a lot of work off your network and security teams' hands.