tufin The Security Policy Company.

Securing Your Network for the New Normal: Accelerate Decision-Making & Response Time via Automation

Digital transformation, which happened practically overnight, is the new reality. As organizations venture into the post-COVID world, they're looking to bridge the divide between processes and workflows that once worked (and worked well), and those that need to be adapted to 'fit' the new normal.

The 'new normal' involves complexity which beckons security policy automation. Network and security teams now face applications operating beyond the perimeter, user movement outside the perimeter, and an increase in network heterogeneity. This has resulted in a more fragmented network and a significant surge in the number of firewall or firewall-like solutions that organizations need to manage. Network and security professionals must now handle a wider scope of tools, operations, and knowledge to complete their jobs. It's impossible for any one individual to be an expert on all of these technologies and platforms. Organizations require automated, unified and centralized management to control who can talk to who and what can talk to what, to keep up with the scale of these changes.

We recently conducted dozens of conversations with cybersecurity leaders to learn about their handling of the shift to remote working, implications on their network's security, the solutions deployed, and what's next. In this guide, you'll learn about the actions and recommendations we've repeatedly come across, to help you adapt to changing environments, and better prepare for unexpected future events.

How have companies dealt with the 'overnight' shift?

COVID-19 caused a dramatic shift in how companies operate. Based on a survey of large organizations, in early March, numerous companies had to increase the size of their remote workforce by a factor of 5 to 7 in just a few days. One large bank went from 5,000 to 40,000 remote employees, while many organizations now have over 90% of their workforce working remotely.

The existing challenges network teams already faced were now compounded with an additional set of obstacles, namely, having to deal with a dramatic increase in the number of access change requests to accommodate the overnight shift. The demand for speed prevented these organizations from following all of their security practices or even leveraging some recently acquired technologies.

The Quick Shift: KEY FINDINGS

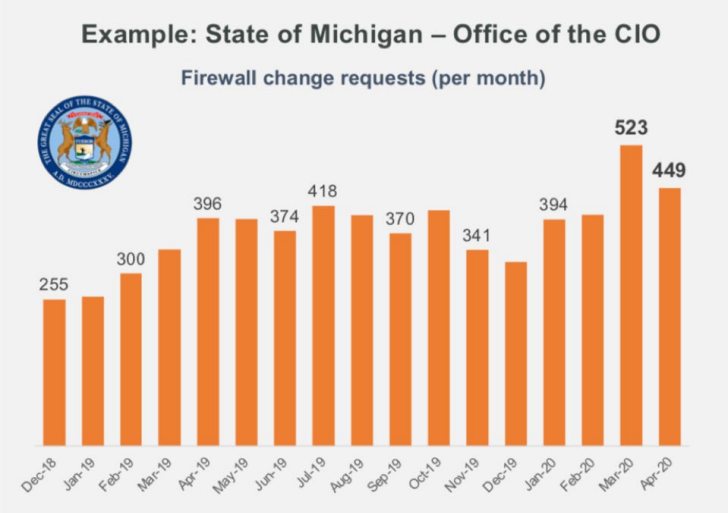
5-7x
increase in remote users

>90%
of employees work from home

A dramatic increase in
network change requests

Most IT departments relied on existing, well-established technologies to enable remote access. Companies deployed their on-premise, existing remote VPN solutions, while others used remote access VPN solutions offered by their firewall vendors. In addition, many used remote virtual desktop infrastructure (VDI) technologies for a small portion of their employees.

To enable traffic, admins had to quickly update network security devices and firewalls with the new IP pools of their employees. Further, some organizations set up additional VPN gateways to meet the required traffic capacity.



Office of the CIO for the State of Michigan: orange bars represent the number of access change requests per month, showing a **30-50% increase** in March.

The Quick Shift: KEY FINDINGS

Technologies Used:

Rely on legacy and existing technologies (VPN, VDI)

Implementation:

- Increase the IP pool size/create additional pools
- Users were provided with the same access permissions in each pool

Result:

Flat network, minimum segmentation, permissive access, and increased attack surface

VPN: The #1 technology to enable access

Changes to the infrastructure took place very quickly, often without standard security and risk reviews. Most organizations changed their VPN configuration to increase the IP pool or created additional pools to accommodate all users' access needs. By deploying a small number of remote access IP pools, all connected remote employees were granted the same internal network access to resources.

What was surprising, however, was that even organizations that had upgraded to next-generation firewalls (NGFW), did not use them to provide better security and control for remote users connecting via VPN. Presumably, this was due to the fact that they could not easily nor quickly enough translate NGFW policies to other legacy network security devices for end-to-end policy enforcement.

Bypass controls to quickly enable access

Because changes were made fast, the easiest way to enable quick access, was to grant access, regardless of an employee's role and "normal" permissions level. Further, most of the changes implemented did not follow standard change procedures and evaluation, and were not fully documented. What's more, many changes were performed manually, leading to a higher probability of human error and misconfigurations.

As a result, access control was left to application-specific user permissions and authentication. Essentially overlooking segmentation meant enabling easy network access and lateral movement for an intruder. More important, this goes against good security practices. To accommodate the changes for the remote workforce, security postures have been weakened, while attack surfaces have increased due to additional unnecessary access.

Three Fundamental Steps You Can Take Today

Based on discussions with several CISO and senior cybersecurity leaders, the most successful approach across the board, is to first define and then carefully adhere to a solid actionable and workable framework based on three distinct practices.

Securing Your Network for the Remote Workforce: Basics Checklist

1 Identify, assess and prioritize risks

To improve the security posture, organizations generally agree that the first priority is to identify and assess security gaps and prioritize the risks. The changes that were made quickly need to be reevaluated to reduce risk, prevent audit issues, and restore compliance. This will enable you to get a head start on your recovery efforts.

✓ **Identify what changes were made, by whom, the reason for the change, and visibility of the type of network access remote employees now have.**

TIP

Tufin Object Change Report https://tinyurl.com/y2ola474 provides instant visibility by device, security group or timeframe. Here, you can view a list of the changes made to objects - services, users, and network objects. This report flags the exact moment an object was changed and by whom, and alerts on sensitive changes with critical objects.

✓ **Determine if all access changes were necessary. For higher risk zones or assets, determine if there is a business justification for the access, and if access rules are being used.**

TIP

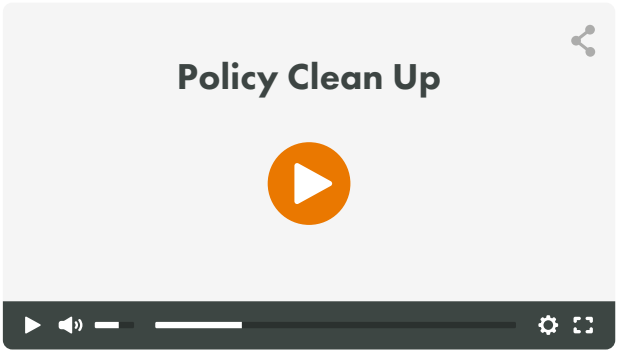
Tufin Rule and Object Usage Report https://tinyurl.com/y2yhrvvr provides statistics on the most/least-used and unused rules and objects. Here, for each rule or object, you can view the number of logged network ('rule hit') traffic that was passed or blocked. You can use this report to optimize your rule base by identifying which rules are not being used and therefore should be considered for removal, and which rules are heavily used, and therefore should be moved up in the rule base. Unused objects should also be candidates for removal.

In addition, you'll probably want to look for rules with expiration dates or where the comments section is left blank after aparticular date. This will help to identify and assess rules that may be overly permissive.

Assess the risk of changes. Measure access rules against your organization's security policy to ascertain impact on compliance.

TIP

Tufin SecureTrack (https://tinyurl.com/yxttzkw8) provides risk assessment, permissiveness level checks and rule change validation against your segmentation policy. Here, you can set your policy and gain visibility into all firewall changes across your multi-vendor, hybrid network. You can view policy violations which are detected based on, for example, rule hit, zone changes, or anomalous port-specific network behavior. Once violations are detected, you can go ahead and make modifications and changes to rules using Tufin SecureChange to reduce risk.



Watch this short video (7 min.) (https://tinyurl.com/yxs7ymex) to learn how to quickly and accurately clean up your network policy from fully shadowed rules.

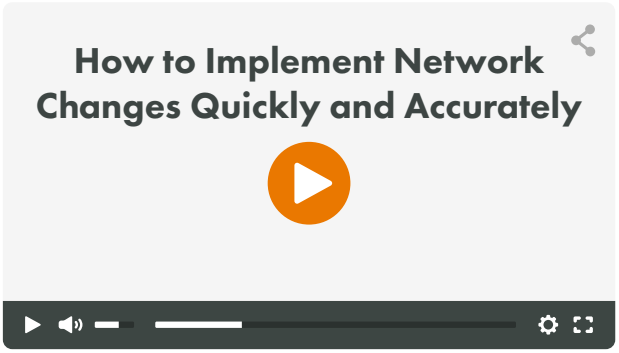
2. Execute quick fixes for fast and effective mitigation, while maintaining business continuity

Once risks are assessed, security policy best practices are recommended. Following is a list of quick improvements that can be easily made to help you improve your network security posture without hindering business continuity.

Reevaluate risky access changes to determine if all changes were necessary, to assess if there is business justification to the access, and if all access rules are actually being used. This ensures changes that involve sensitive assets/zones go through the risk analysis, verification and approval processes you defined.

TIP

Use Tufin SecureChange to simulate the change and conduct impact and risk analysis to confirm alignment with your organization's security policy, either as a standalone step or as part of the Access Change Request workflow.



Watch this short video (4 min.) (https://tinyurl.com/y3nxpvmx) to learn how to use Tufin SecureChange access request workflow to implement network changes quickly and accurately.

Tighten remote access policies by executing rule optimization or clean-up

Replace overly permissive rules, where overly permissive is defined as allowing access that is unused, with more granular rules. This helps establish least privileged access, ensuring remote users are granted only the access they need.

TIP

Tufin Automated Policy Generation (APG) (https://tinyurl.com/y2n9or3g) inspects actual traffic flows and recommends a set of rules/objects to reduce the permissiveness of the existing rule. APG can process weeks or months of log data from any of the leading firewall vendors.

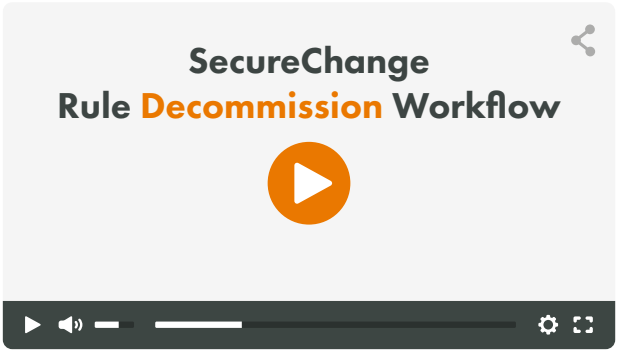
Decommission unused or redundant rules that may have been implemented in haste when enabling remote employee access, or due to not knowing what access was actually required at the time changes needed to be made.

TIP

Tufin SecureChange provides unlimited, customizable workflows to help you automatically design, vet and implement network access changes.

You can use **Rule Decommission workflow** (https://tinyurl.com/y6ze78a9) to decommission unused, overly permissive rules, or **Rule Modification workflow** (https://tinyurl.com/y4fygnve) to execute changes in existing rules while maintaining business continuity.

Watch these short videos (~2 min. each) to learn how to use Tufin SecureChange to modify or decommission rules



(https://tinyurl.com/y6ze78a9)

(https://tinyurl.com/y4fygnve)

Create basic remote access segmentation policy to differentiate between remote users based on roles/groups/locations. This will help you apply the same segmentation principles for remote users that is utilized in the on-premise segments.

TIP

Tufin provides ready-to-use segmentation templates that are based on predefined zones to help you set allow/block traffic for specific zones and AppID.

From \ To	DMZ	Internal Network	Internet	Third Party Network	Unassociated Networks	VDI Access - Citrix	VDI Access - VM Horiz...	VPN Users
DMZ	✓	⊘	⊘	⊘	⊘	⊘	⊘	⊘
Internal Network	⇄	✓	⊘	⊘	⊘	⇄	⇄	⇄
Internet	⊘	⊘	✓	⊘	⊘	⊘	⊘	⊘
Third Party Network	⊘	⇄	⊘	✓	⇄	⊘	⊘	⊘
Unassociated Networks	⊘	⊘	⊘	⊘	✓	⊘	⊘	⊘
VDI Access - Citrix	✓	⇄	⊘	⊘	⊘	✓	⊘	⇄
VDI Access - VM Horiz...	✓	⊘	⊘	⊘	⊘	⊘	✓	⇄
VPN Users	✓	⇄	⊘	⊘	⊘	⇄	⇄	✓

3. Planning for the future – long-term considerations

Improve security posture by applying more granular segmentation policies (e.g. based on UserID)

Create more granular segmentation policies by leveraging user identity technology with NGFW. This enables you to apply network security policies based on identity and context and less on IP addresses, to allow user access from anywhere.

Apply rule recertification processes

Apply proper recertification processes to all modified firewall rules to ensure firewall rules are regularly recertified and are still needed by the organization.

TIP

Tufin SecureChange Rule Recertification Workflow (https://tinyurl.com/y2enn57u) can help you streamline the rule recertificate process by fully automating the process of tracking, monitoring and managing the expiration of firewall rules. Tufin automatically identifies expiring rules, provides visibility into rule metadata, and enables automatic recertification across vendors and platforms to help you maintain continuous compliance and simplify audit preparation.

Automate manual processes to enable fast and accurate changes

Nearly every network access change involves complex implementation throughout multiple, multi-vendor firewalls, switches, and routers, as well as security groups. Performing these tasks manually, renders it impossible to handle tickets in a timely manner without exposing the network to potential risks. Even if only 60% of your changes are automated, this will result in substantial time and cost savings.

> Through 2020, **99% of firewall breaches** will be caused by firewall misconfigurations, not firewall flaws.
>
> One Brand of Firewall Is a Best Practice for Most Enterprises, Gartner

TIP

Use **Tufin SecureChange workflow configuration** (https://tinyurl.com/yyeehsl9) to set workflows that automatically streamline every step in the change process, ensuring fast, accurate, and documented access change processes. This will help you remove bottlenecks in your daily operations, and eliminate the risk of configuration errors. SecureChange ensures every policy change is evaluated for security impact, and then automatically implemented across your hybrid, multi-vendor network. Workflows are fully customizable.

Watch this short video (4 min.) (https://tinyurl.com/yyeehsl9) to learn how to use Tufin SecureChange to create workflows that can streamline the network change implementation process and help you meet the specific needs of your organizational processes.

Today, in such unique circumstances, more than ever, organizations have to do more with less – manage resource shortages, react quickly, and address changes and issues in a rapidly changing environment. It becomes critical to have clear, well documented and repeatable processes with minimal manual intervention. By implementing proven, highly secure practices to accelerate change processes today, your organization will be primed and ready to handle the next crisis.