tufin

Tame the Network and Security Challenges of a Data Center Migration

The Tufin Orchestration Suite™ is essential to a well-planned, well-executed migration

Introduction

Data center migration plans are high on the list of key projects for many CIOs these days. Migrating company applications from one location to another, or from one platform to another, represents a lot of risk for an organization. Still, many companies undergo the arduous process with the expectation that it will result in significant efficiency and business agility.

There are numerous reasons why companies undergo a data center migration. For many businesses, it is part of an IT cost reduction initiative. Data centers, particularly older ones with a 1:1 ratio of applications to servers, are very expensive to operate and maintain. Companies may have obsolete legacy hardware or software platforms that are no longer supported by vendors, leaving them little choice but to migrate to a modern infrastructure. Companies that have gone through mergers or acquisitions may be looking to consolidate multiple data centers into one or just a few in order to eliminate redundancy and to attain the cost efficiencies expected by combining companies.

Another huge driver for data center migrations is to increase business agility by utilizing cloud and virtualization technologies and services that can be quickly provisioned and adapted to rapidly changing business needs. Many companies today are taking their applications out of a traditional on-premise data center and moving them to the cloud—whether it be a public, a private or even a hybrid cloud.

Regardless of the reason a company has, or the destination platform it chooses, data center migration and consolidation projects can offer the opportunity to meet many business needs, including improving the organization's security and compliance posture.

> *"A well-planned migration often becomes a well-executed migration, and a well-executed migration is often much faster, end to end, than one that is run in an ad hoc manner."*
> –David J. Cappuccio, Gartner analyst

Despite the fact that many organizations are undertaking such a major transition, few people in IT today have legitimate experience going through an entire migration project. People who did the hands-on work during the last great migration period – the one that led companies from mainframes to client/server computing – have mostly retired or moved on to other roles in their organizations. As a result, their knowledge and experience in how to plan and execute a complex data center migration is lost to history.

According to Gartner, 70% of data center migrations will incur significant time delays or unplanned downtime, largely due to improper planning. This figure is based on more than 300 client interactions Gartner has had in the past four years in which data center migrations were discussed.[1]

[1] David Cappuccio, Gartner, Inc., "Data Center Migrations – Five Steps to Success," 26 March 2014

A data center migration is an exercise in risk mitigation. It takes superior planning and execution to make the transition in a timely fashion and with little to no business disruption. Gartner analyst David Cappuccio wrote: "A well-planned migration often becomes a well-executed migration, and a well-executed migration is often much faster, end to end, than one that is run in an ad hoc manner."[2]

The data center security policy layer is often the most challenging to replicate between data centers and even cloud environments. These policies are the central nervous system of an organization's entire data center, which makes policy analysis and configuration control absolutely essential throughout the migration process.

The company that wants to ensure a successful migration will take advantage of tools that automate the process of planning for, predicting and testing the impact of changes to security and network devices, even before those changes are actually made. This white paper looks at how the Tufin Orchestration Suite helps companies discover their applications and the associated dependencies, as well as plan, predict and execute changes at the network security layer of their data center migration.

Data Center Migration Challenges

A large scale migration project can be one of the most risky and complex undertakings an enterprise can experience. The challenges are myriad, but there are three universal challenges inherent in every migration project.

Discovery of Application Dependencies

The organization must fully discover all of the application service dependencies, even for applications that are not considered part of the migration project because they can have unknown or undocumented relationships and dependencies.

If a server is being moved from data center A to data center B, or from physical server A to virtual server B, there are many components that depend on that server. For example, perhaps there is an application running on that server and there is another secondary application that communicates with a database which is on this server. If the database is going to move elsewhere, then the secondary application is going to stop working because the application code has it hard-coded somewhere that the database is located on a specific IP address.

Closely related to this issue is the need to identify business ownership of the applications. It's common that many applications currently running in an organization's data center have been running there for many years. The people who know the details of these applications might not even work for the company anymore. It's not that unusual to have an application where no one really knows precisely how it is working. This isn't terribly important as long as everything is working as expected, but if there's a stoppage for any reason, the application owner will want to know why.

[2] Ibid.

It's quite hard to understand what applications exist and what dependencies they have in the network. In many organizations the configuration management database (CMDB), which should contain an accurate version of this information, isn't actually up to date. At the same time, this is critical information to have because without it, the organization has a big risk of having business downtime.

Gartner says this discovery and identification phase is really a risk-assessment phase and it's one of the most important stages of the migration planning process. It entails doing a detailed evaluation or audit of exactly what needs to be moved, when and how. David Cappuccio of Gartner writes: "This phase takes a detailed look at applications, network requirements, and most importantly, dependencies between applications and the cascade effects on application delivery and business impact if an application fails to migrate correctly."[3]

Minimal Impact on Business During the Migration

The ideal scenario is to be able to migrate all necessary hardware, software, applications and services with no discernible impact on business operations. This includes making the required changes to the network and security policies. The people who are doing the migration are typically given scheduled periods of time in which they are expected to complete all necessary work. Failure to adhere to this window of time might have a negative impact on business and would certainly reflect poorly on the competence of the migration team. Consequently, the team members need to have better predictability in the process of moving things from one platform to another, as well as a good level of certainty that they can accomplish what they need to do in the allotted time.

For instance, the team might be given a four-hour window to cutover business operations from an application that has been running in a legacy data center to a parallel application that is running in the cloud. The migration team expects their work should take less than four hours but they want to allow extra time in case problems arise. Before doing the cutover, they look for ways to shorten the migration process and also to have more certainty in predicting what work is required for this critical process. During the migration, they want to have good visibility and control so they know exactly what's going on.

Security, Risk and Compliance

While the entire migration process is fraught with risk – what if something goes wrong and business is disrupted? – the more long-term concern is about risk and security issues that might be introduced as applications move from one platform to another. For example, in moving from a legacy data center to a virtualized environment, physical firewalls may give way to the virtualized version, which may be something the operations team is not yet completely comfortable with. The challenge for the migration team is to make sure that, as they are moving things around, they are actually improving the organization's security posture and they are not adding new risks to the mix.

---

[3] Ibid.

With regard to the network aspect of the new platform, the team is especially concerned about risks from misconfigurations and from policies not being fully implemented or even up to date. A firewall change to enable connectivity of an application that has been migrated from one environment to another is a potential risk to security and business continuity. For example, it's not uncommon for security and networking teams to first focus on enabling connectivity in the new environment in order to make sure the business applications are working. For this they often configure their firewall and routers with an over-permissive security policy which focuses on connectivity rather than security. They plan to go back later and "fix this" but unfortunately they never get around to tightening their security policies. Consequently they end up with a more vulnerable network.

Migration teams need visibility into how making such changes will impact everything else. Now consider that a data center migration can easily involve hundreds or even thousands of applications and the magnitude of the challenge becomes quite large.

Maintaining compliance is another issue. Every business of a significant size is compelled to comply with at least one government- or industry-mandated regulation, whether it be the Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley, the Gramm-Leach-Bliley Act (GLBA), the Health Information Portability and Accountability Act (HIPAA), or any number of others. Companies often have internal regulations as well. The regulations and standards relating to information security put an emphasis on compliance and the regular auditing of security policies and controls. While regulatory and internal audits cover a broad range of security checks, the firewall is featured prominently since it is usually the first line of defense between the public and the corporate network.

The task of maintaining compliance is difficult, at best, in a multi-vendor environment, and the additional burden of migrating from one platform to another compounds the challenge of adhering to regulatory requirements. Once again, this process requires good visibility before, during and after the migration.

Technology Challenges

One of the great benefits of a new data center are the new technologies that are being implemented today, whether it's cloud, virtualization or SDx ("software defined anything"). These technologies offer tremendous flexibility which helps an organization gain business agility. Now it's possible to adapt the computing infrastructure quickly to meet changing business needs. Nevertheless there are some general technology challenges in a migration project.

Automation

The new technologies enable automation because they are programmable. They offer application programming interfaces (APIs) to program or provision resources automatically using software. In virtual environments, for example, new server instances and their associated security applications (such as firewalls) can be spun up or shut down based on thresholds that are programmed into business applications. This can happen multiple times a day for applications that have peak periods throughout the day. For instance, a stock

trading application can experience high volumes at the opening of the market for the day, as well as just before the close of the market. Provisioning automation that is tied to peak trade volumes is possible in a virtual environment whereas it couldn't even be imagined in a legacy data center.

Automation can be a boon to productivity but it also is risky. If network resources can be automatically provisioned from a portal or an application, then how can the organization ensure that this network or the other things that are changing are not introducing new risks or are not breaking compliance in the data center? This is a big challenge for security operations.

Virtualized technologies can throw compliance for a loop as well. Those responsible for auditing the organization's compliance posture must have visibility in the new technology environment.

Choosing "the Right" Technology

The good news is that there are a lot of very good cloud, virtualization and SDx technology choices that can take companies well into the future. Numerous vendors offer competing technologies that provide similar capabilities albeit slightly different approaches. The bad news is that there is no obvious answer as to which technologies are "the right" choices. Many companies are trying to make the technology decision that is right for their company and that won't take them on a limited path.

Security

Things move very quickly with regards to the new technology platforms. When an organization migrates to a virtualized data center or to a cloud platform, it's expected that the technology will change and adapt to business needs as they arise. Contrast this to a legacy data center where even a small change could take weeks or months to plan and implement.

Such rapid changes don't bode well for maintaining tight security. The appropriate policies need to be defined to fit the business needs of the new data center, but the security operations team needs to know that the policies will be secure and they won't be adding any new vulnerabilities. This team would surely like to have more time to consider the impending changes, but they don't have the luxury of time; they are expected to be as agile as everyone else in this game.

Legacy Systems

A migration to any new platform takes time, and during this time the organization will have both the legacy and the new data centers operating in parallel for a time—possibly even years. The company needs to maintain both infrastructures and have visibility and control over what is going on in both environments, preferably from a single point of control. Moreover, it would be great to bring some of the operational efficiencies of the new platform back home to the legacy data center while both environments are in operation simultaneously.

The Migration Challenges Create a Gap

The challenges outlined above create a number of risky "unknowns" that can derail the migration plan. It might be difficult for an enterprise to know about or determine all of the network dependencies of its applications, regardless of whether or not those applications are slated for migration. Given that the organization will have a limited amount of time to migrate an application from one platform to another, it can't tolerate having these unknowns in the plan. This would certainly risk having unplanned business downtime and that just isn't acceptable to anyone.

Of course, making any kind of changes to the networking and security devices that support and protect the organization's applications introduces security and compliance risks. This is especially true when the new platform involves automated provisioning and deprovisioning of virtual servers and other resources. The enterprise must ensure that making changes to firewalls and other security solutions does not compromise the organization's security and compliance posture.

During and after the migration, the organization will need visibility into and control over the old as well as the new environment as they work in parallel for however long is necessary. These things can't be done manually. Most enterprise networks are simply too large and too complex and they aren't well documented. Most companies have insufficient on-staff or contracted resources to do the tedious work of discovery, mapping, risk analysis, monitoring and more—on two platforms, not just one. Moreover, the people might not be skilled on all the technologies, new and old.

This leaves a gap in what must be done and what realistically can be done to plan, execute and fully wrap up the migration with minimal impact on the business. The gap sits between the organization's applications, whether commercial or homegrown, and the network infrastructure layer which the applications run on. This gap is illustrated in Figure 1.

Figure 1: The gap between applications and network infrastructure

The Tufin Orchestration Suite Fills the Gap

The Tufin Orchestration Suite fills this gap by automating the network change process for enterprise applications. The suite is comprised of several components that interact with each other as well as with the network infrastructure and the business applications. The suite also supports APIs to communicate with other important elements of the computing environment. The architecture of this suite is illustrated in Figure 2.

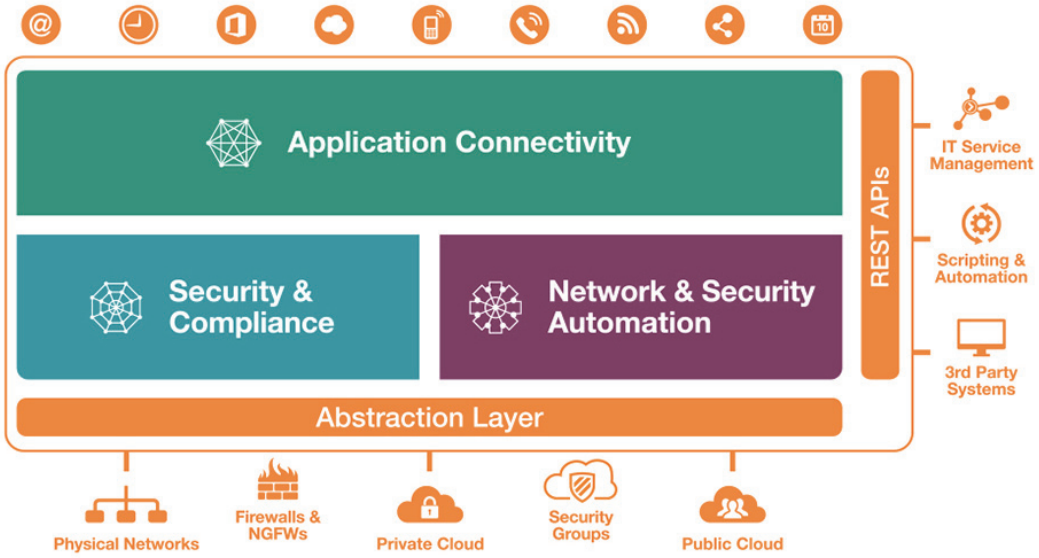

Figure 2: The architecture of the Tufin Orchestration Suite

Briefly, here's a description of what each of these components does.

- The ***Business Application & Services*** component allows an organization to model its business applications and services, defining the network resources they require in order to work.
- The ***Security & Compliance*** component holds the organization's Unified Security Policy (USP). The USP defines the desired (or required) security policies that must be enforced in the organization. These include segmentation policies, best practices policies, regulatory compliance policies (such as PCI, SOX, etc.) and any other security policies the organization wants to comply with internally.
- The ***Network & Security Automation*** component enables change automation in the network. This component performs the actual security automation activities, while checking with the *Security & Compliance* component that these automated changes are not breaking or violating the desired security and compliance policies.
- The ***Network Abstraction*** component hides the network complexities from the other components. It maps and holds the network topology and interacts with the different networking and network security technologies running in the network.
- The ***RESTful APIs*** component enables full programmability to any of the suite's components, allowing easy integration with other enterprise systems and technologies.

How the Tufin Orchestration Suite Addresses the Migration Challenges

Let's look at how the Tufin Orchestration Suite addresses the general and technology migration challenges identified earlier.

Discovery of Application Dependencies

The challenges for the migration team are to discover and identify all application network dependencies, and to identify business ownership of the applications.

The Tufin Orchestration Suite addresses these challenges with numerous capabilities, one of which is automatic application discovery. Tufin builds a repository of all an organization's applications, documents the applications' requirements from the network, and displays their current connectivity status. To speed up the process of documenting connectivity for existing applications, Tufin provides automatic connection discovery. This feature analyzes an organization's firewall revisions and network traffic to reveal the communication paths associated with servers, including relevant ports, and possible sources and destinations. By defining one server, Tufin can reveal all of its connections.

Taking this a step further, Tufin's application modeling capabilities allow an organization to define and maintain dependencies between applications and services in order to understand how changing one application server affects other applications. This is especially important in a migration scenario where moving an application server to a new platform can have far-reaching ramifications. The migration team can model the application move to see what impact it will have before actually making the change, and then Tufin can automatically provision the network to accommodate this change if desired. This enables the team to plan for and take the necessary actions while reducing the risk of overlooked dependencies.

Another follow-on to the application discovery feature is that the Tufin Orchestration Suite documents the rules in firewalls and other security devices, including the reasons for the rules. This helps the organization know which rules are enabled for which applications, and why, which is important when applications are being decommissioned or migrated.

The Tufin suite also helps an organization determine if rules or objects defined in the firewalls are actually being used, and this helps in modeling the new data center. For example, if there is a rule that is documented to serve a specific application and it is observed that there is actually no traffic going through that rule, it typically means this application has not been using the rule or this application is no longer living there. Thus, either the application has changed and therefore the rule needs to reflect the application and network dependency, or the application has been retired and the firewall has not been updated to reflect this retirement. Such data can help the migration team understand what sort of applications are really being used and how often they are being used, and this enables them to better model the new data center.

Another Tufin feature that can be used to better identify an organization's applications and network dependencies is a network topology map that is automatically generated to increase visibility of the network abstraction layer. This interactive map of the network enables the migration team to see how traffic is moving from point A to point B; what routers or other network elements the traffic is going through; and whether or not the security policies running on those network devices will allow the traffic to pass through.

From a business ownership perspective, the Tufin Orchestration Suite documents all of the information discussed above. At any given moment the migration team can draw what the

current scenario is, and pushing it forward the team can gain more and more insight that can be useful in staging the migration phases.

Minimal Impact on Business During the Migration

Recall that in order to meet this challenge, an organization would be looking for a shorter migration process, predictability in what needs to happen, and visibility and control. The Tufin Orchestration Suite provides a range of capabilities to ensure that there is minimal impact on the business during the migration process.

In any migration, it's critical to have a well-defined workflow process. Tufin provides workflow process automation, which is the ability to define and carryout the workflow of how change needs to be implemented. For example, an application migration process requires a business approval and risk assessment before doing the actual implementation. By automating this process, it's less likely that mistakes will be made and it's easier to track the progress of the various tasks and know how long the overall process will take.

As part of the workflow process, the Tufin suite has specific commissioning capabilities for migrating applications as well as services for decommissioning. Tufin can automate the network security part of those actions, to change the firewall and router configurations for the migration or to fill whatever holes opened up in the firewall to begin with as services are decommissioned. This saves a lot of time and reduces errors versus performing the tasks manually.

Tufin delivers an application management capability to aid with automation. The tool can be used to model an application and then automate changes to the application. For instance, an organization can model an application and specify that it requires connectivity to server A. Now the server is moving, so an administrator can go into the model and change server A's IP address to a new one. Tufin can then analyze the proposed change for risk before provisioning the network automatically and making all the necessary changes.

The Tufin solution has continuous monitoring for application connectivity visibility as part of the application modeling capabilities. By tracking its applications, an organization can easily see what is dependent to have these applications work properly. If a change on the network breaks a necessary connection, Tufin can send an alert to notify an administrator of the problem. There's also an ability to simulate what is going to change and what is going to happen, which is extremely helpful in designing the migration without trial and error.

Security, Risk and Compliance

The challenges here are to improve the organization's security posture without adding new risks; maintain compliance with policies and regulations while things are moving; and gain visibility into the security and compliance posture.

Gaining control of network security is difficult given the complexities of today’s enterprise networks. A good security posture dictates a well segmented network, protecting the more sensitive assets (such as cardholder data) from the less sensitive assets, often using firewalls. Many organizations manage network segmentation by manually tracking firewall

and router configurations on spreadsheets, but with constant change requests coming from the lines of business, maintaining the desired/required network segmentation is practically impossible.

Within the Tufin Orchestration Suite, the Unified Security Policy provides the ability to centrally manage all of the organizational security policies in a single place. Unified Security Policy automates the complicated process of managing policies, the complex rule bases and a constant influx of change requests for multi-vendor/multi-technology networks. Unified Security Policy controls the actual versus desired network segmentation, highlighting policy violations before a change is made on the network so as not to break compliance or expose the network to unnecessary risk. It ensures that all future changes in the network are aligned with the centralized policies and any new violations introduced to the network are alerted on.

Unified Security Policy gives a simple visual representation of the network segmentation across a multi-vendor array of firewalls and routers existing across an organization's network. Figure 3 shows the user interface of the Unified Security Policy.

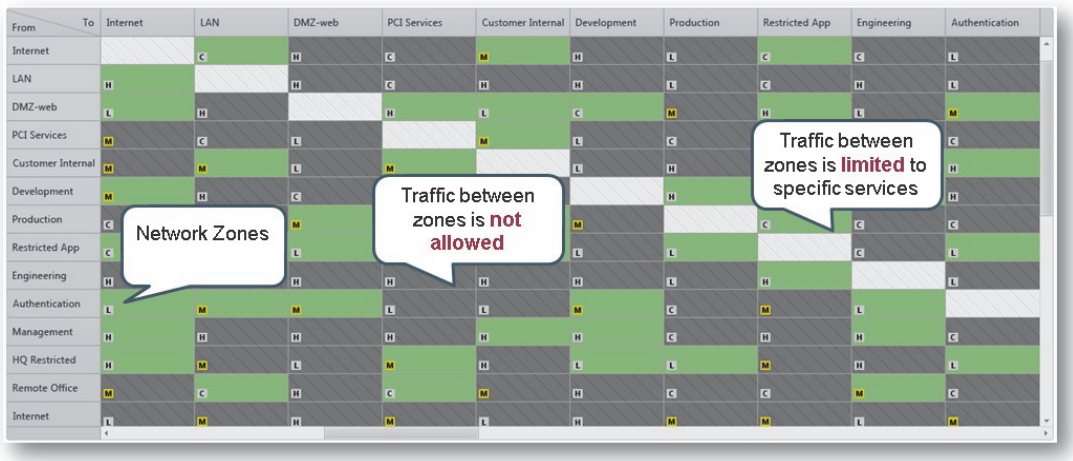

Figure 3: The visual user interface of the Unified Security Policy

Using Unified Security Policy, an organization can do a risk analysis on an application at any given time. For example, the migration team can map out an application which requires connectivity to different assets in the network. Once there is a model of this application, Tufin can determine if the model is breaking the organization's compliance posture, or if it is introducing a new risk; for example, breaking the organization's network segmentation policy. Perhaps someone is trying to connect a "PCI zone" to a "non-PCI zone" without even being aware of the required segmentation. All of this can be simulated and assessed for risk and compliance before the action is really taken. In the event that a change was made without a pre-change risk assessment, and the change created a problem in the system, Tufin can alert on the problem and provide details about the conflict in policies or conditions. This risk assessment as part of change management is a powerful capability to have for a migration process when so many aspects of the network are in flux.

All of the device changes made through USP are fully documented, and there is a complete audit trail to aid with compliance validation. In addition to the USP single-pane-of-glass dashboard, administrators can generate reports on demand to see the status of all monitored devices.

As an example use case, the largest public cloud provider and managed security service provider in Switzerland is using Tufin Orchestration Suite as an end-to-end automation tool for its entire Check Point infrastructure consisting of about 120 physical firewall gateways hosting more than 200 virtual firewalls. Rather than managing policies in each of the individual firewalls, the service provider used Unified Security Policy to create a central object repository for the policies for all of the devices. The rules are then pushed out to the firewalls but managed centrally.

At this writing, this company is building a new data center facility that will utilize about 360 virtual firewalls from both Check Point Software and Stonesoft (now part of McAfee). The Tufin Orchestration Suite will be instrumental in maintaining security and compliance while migrating existing applications to the new data center and for centrally managing the devices on the new platform long-term.

Choosing "the Right" Technology

Some of the new data center technologies are still evolving. Various vendors have their own implementations of similar technologies, and they aren't necessarily compatible with each other. Enterprises may give many of the technologies a try before settling on a final path.

Tufin recognizes there are all types of technologies under the network abstraction layer, and we take a vendor-neutral approach to them in order to support as many technology approaches as possible, as shown in Figure 4. Today Tufin supports solutions for traditional networks, private clouds, public clouds, and software defined networking, and more solutions within these categories are on the roadmap. This gives enterprises the comfort of knowing that the Tufin Orchestration Suite can manage security and networking devices in a range of data center scenarios.

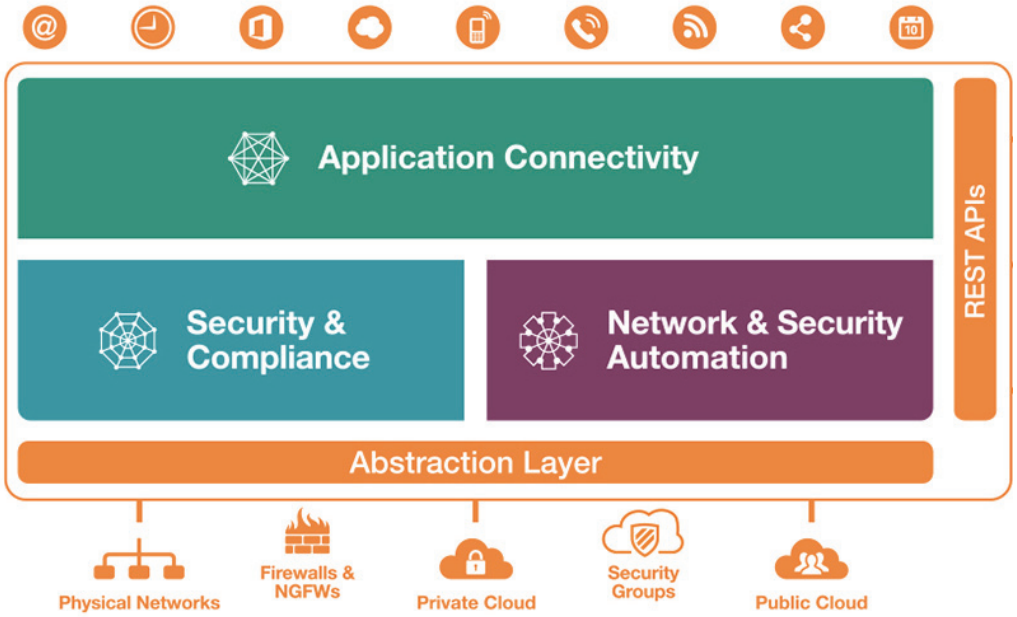

Figure 4: Tufin supports a range of technologies under the network abstraction layer

Legacy Systems

The transition to a new data center takes time—months and possibly even years. This means there will be a period of time when an organization is operating in two environments, one of which has vibrant new technologies and the other which has legacy technologies. With regard to the networking aspects

of the legacy data center, is it possible to bring some of the operational efficiencies of the new technologies to the legacy technologies?

The Tufin Orchestration Suite makes it possible with automation that is similar to software defined networking (SDN). Tufin provides SDN-equivalent capabilities to existing non-SDN network security technologies. Tufin can automate changes in the network, automatically designing a change in order to address a specific business need, and also automatically provision or implement the change without any manual interaction. Tufin also provides APIs to allow other enterprise systems to use these abilities.

The Unified Security Policy capabilities work across legacy platforms. This enables the software defined data center (SDDC) promise of enhanced security and agility through a trusted, automated and multi-vendor management platform. An organization can implement a consistent policy across the entire network with each platform enforcing it at its own level.

Conclusion

A data center migration is no simple project, especially when it involves a wholesale change in the underlying infrastructure technologies, such as from legacy to cloud or virtual technologies. The migration can be fraught with risks unless it is well planned, the changes are assessed for risks before they are implemented, and policies and controls are aligned across all platforms and devices.

Tufin streamlines data center migration projects for minimal business disruption and maximum security control. The Tufin Orchestration Suite accelerates application migrations and ensures security and compliance in three important ways:

Application management and discovery – Tufin simplifies application migrations with end-to-end application management. This includes rapidly discovering applications based on network traffic and policies; managing application dependencies and business ownership across the data centers; and maximizing control with application visibility.

Minimal impact on business – Tufin helps to minimize the impact on business during the migration with automation and control. The Tufin Orchestration Suite improves visibility and control with workflow process automation; provides real-time alerts on network changes that impact application business continuity; offers full automation for application and service migrations; and increases migration predictability and control with network and security policy automation.

Security & Compliance – Tufin helps organizations boost security and compliance with "baked in" security controls. Companies are able to centrally manage compliance standards and policy violations across data centers and get full accountability and auditability for any security configuration changes. Real-time alerting on security and compliance violations helps to keep problems in check. Clear visibility into security violations and risks helps organizations do better application architecture planning. In addition, an organization can maximize ongoing control with integrated security checks as part of the change process.

If your organization is planning or in the midst of a data center migration project, talk to a Tufin representative to learn how Tufin Orchestration Suite can facilitate your project planning and execution. You can even try the Tufin solutions for 30 days for free.

About Tufin

As the market leader of Security Policy Orchestration, Tufin automates and accelerates network configuration changes while maintaining security and compliance. Tufin's award-winning Orchestration Suite™ gives IT organizations the power and agility to automate and enforce security policies across complex, multi-vendor enterprise networks. With more than 1,400 customers worldwide, Tufin enables IT to implement network changes in one day instead of one week, with increase accuracy and security.