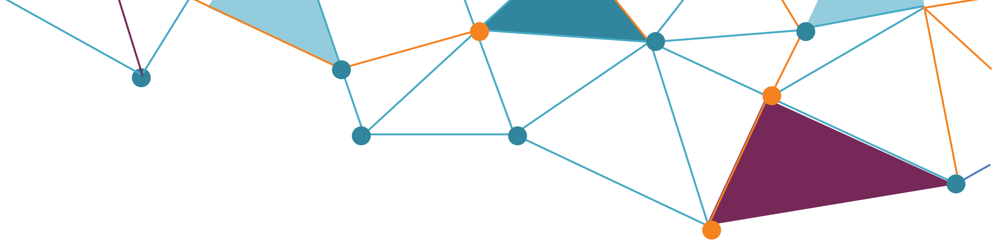


A Survival Guide for Enterprise Security Policy Compliance

How to Stay Compliant with
Regulatory Cyber Security Standards
and Organizational Policy

www.tufin.com

It's a Jungle Out There

Every business operates within the context of risk. The risk might be in the form of a tenuous supply chain, geopolitical concerns, upstart competition, or any number of issues specific to that business. Certainly the risk associated with cyber security has a big spotlight on it today—so much so that cyber security has become a Board-level topic of interest for many organizations.

There are numerous guidelines and regulations to guide companies toward mitigating their cyber risks: ISO/IEC 27002, the NIST Cybersecurity Framework, PCI DSS, and so on. It's essential that organizations put controls in place to protect their digital assets. Change management is an important aspect of these controls, as business needs will dictate frequent changes to the digital infrastructure.

Compliance with cyber security regulatory requirements has transitioned from a "check the box" mentality to a stringent program whereby the requirements are diligently met, continuously enforced and proven through regular audits. Many companies' change management programs now consider "what if" scenarios to guard against policy violations before a change is approved or implemented.

Strong cyber security starts at the top, with well-defined policies designed to mitigate the business risks. From there it moves down into operational areas such as IT where network security professionals are charged with creating, maintaining and continuously enforcing a long and complex set of rules that control how the networking infrastructure operates within the constraints of the regulatory and internal policy mandates. The goal is to ensure the enterprise network keeps pace with the business while allowing it to operate within an acceptable level of risk.

This is quite the herculean task, given the extreme complexity of the typical IT infrastructure today. Most, if not all, large enterprises have a multi-vendor, multi-technology heterogeneous environment which often includes physical data centers as well as virtualized private cloud and public cloud platforms. What's more, as enterprises bring in new networking technologies – VMware NSX, as an example – they continue to operate their legacy systems for many months and even years. On the whole, this hybrid enterprise computing environment can be a metaphorical jungle, with hundreds or thousands of physical and logical devices to manage, and with more rules than any human can possibly fathom.

Like the real jungle of the Amazon Rainforest where sunlight barely penetrates to the forest floor, today’s network infrastructure jungle has its own stifling lack of visibility. Network professionals rarely have comprehensive visibility into the security and compliance posture of the hybrid IT environment. Moreover, there's little consistency of how to proactively assess risk and apply policies across legacy, virtual and cloud platforms. This creates a tremendous burden for network security administrators who must use numerous tools and check multiple consoles to do their job.

Yet even with all that complexity across the technologies and platforms, enterprises must still maintain security for data and applications and have the means to ascertain and validate their compliance with regulatory requirements and internal policies. They must ensure that policies are properly designed, applied and maintained across the spectrum of security mechanisms of all devices and platforms--including subnets and zones used in legacy firewalls, application and user IDs in next-generation firewalls (NGFWs), micro-segmentation of SDN solutions and security groups in public and private cloud. It's no wonder that security administrators often feel lost in such a jungle.

Compliance and Audit-Readiness —The Road to Hell?

For the most part, government and industry regulations were born out of a genuine need to protect valuable applications and data, and to ensure continuity of service. Certainly that's a good thing. But as the saying goes, "The road to hell is paved with good intentions."

Oftentimes enterprises must operate under the requirements of multiple regulations and security standards. The speed and breadth of change of these requirements is quite a challenge for those who must interpret and apply them. According to the 2015 Thomson Reuters Annual Cost of Compliance Survey, 70% of the responding firms are expecting regulators to publish even more regulatory information in the next year.[1] This leads to "regulatory fatigue"—having too many constraining regulations which can inhibit agility.

Furthermore, for many organizations, the compliance burden is growing but the IT organization's budget for compliance activities is not keeping pace. Forced to do more with less, IT leaders recognize that automation is necessary to get a clear view of the compliance and risk profile from a business application perspective. Unfortunately for many companies, manual processes remain prevalent. The Thomson Reuters compliance survey reveals that 39% of companies are tracking their organization's compliance status in a manual spreadsheet,[2] thus increasing their exposure to risk and the potential for non-compliance with regulations.

Compliance with regulations and internal policy is validated through audits, which in and of themselves can be quite a burden on the IT group. Audit readiness takes time and money—to assemble the required documentation of the current state of the network, and to validate controls through physical tests and attestations. For instance, an auditor might want to examine all firewall rules and test a portion of them to ensure compliance. There can be several audits per year as an enterprise undergoes both internal scrutiny and individual external assessments for separate regulations such as PCI DSS, SOX, and so on. What's more, it's becoming more common today for business partners to require a controls assessment before entering into a services contract. As a result, the audit burden can be quite onerous.

Enterprises can reduce their compliance and audit-readiness burden by maintaining a state of "continuous compliance." That is, attaining a state where all compliance requirements are met, and then continuously maintaining that state. The maintenance portion of this task can be done using automated validation of network configuration changes across all platforms and vendors, and by automatically generating an audit trail. It's easier and less time consuming to maintain continuous compliance than to take a "snapshot in time" approach to compliance. In that case, it's a repetitive effort to bring everything back into a state of compliance every time another audit is anticipated.

Regulatory Challenges

If the truth be told, many organizations are far more preoccupied with ensuring that the network infrastructure supports the necessary enterprise operations and protects sensitive data and applications from cyberattacks than they are with complying with some external regulation. However, compliance requirements should not be ignored or discounted. Government and industry regulations can have some very serious repercussions for those organizations that are out of compliance. Penalties for non-compliance can include increased oversight by regulators, significant fines, and even criminal prosecution and imprisonment in some cases. Executives who sign off on fraudulent or incomplete audit results could have

[1] Stacey English and Susannah Hammond, Thomson Reuters, "Cost of Compliance 2015"

[2] Ibid

personal liability for violations. Consequently, regulatory compliance is gaining Board-level oversight, which increases pressure on IT to ensure that the necessary controls are properly in place.

Owing to their different origins and enforcement agencies, the standards of these regulations aren't harmonized, and from time to time they might even conflict. Organizations are on their own to figure out what standards they must support, and then to translate those standards into rules and policies that dictate how security devices control network traffic. This portends an intimate knowledge of the regulated data, the applications using that data, and the locations of and interactions among the applications. Compliance practitioners aren't necessarily IT-savvy, and IT practitioners aren't always knowledgeable on all the regulations. Achieving and maintaining compliance is a task that's far too complicated to be accomplished without organizational teamwork and technology automation.

Interestingly enough, some regulations intended for a specific geography find themselves as a model for behavior in other regions. The U.S. regulation NERC CIP falls into this category, as many utility companies outside of North America also follow the guidelines of this regulation. And certainly the European Data Protection Reform regulations are a model for data privacy and protection elsewhere around the world.

Table 1 shows just a partial list of the most common government and industry regulations.[3]

Government or Industry Regulation or Standard	Who the Regulation Applies To
DISA STIG – Defense Information Systems Agency Security Technical Implementation Guide	All U.S. Department of Defense (DoD) organizations
FERPA – the Family Educational Rights and Privacy Act	All schools that receive funds under an applicable program of the U.S. Department of Education
FISMA - the Federal Information Security Management Act	• All agencies within the U.S. federal government • State agencies administering federal programs like unemployment insurance, student loans, Medicare, and Medicaid • Any private sector company that has a contractual relationship with the U.S. government, whether to provide services, support a federal program, or receive grant money
GDPR – the General Data Protection Regulation	• The GDPR pertains to all entities that collect, handle or process personal data belonging to residents of the European Union • A secondary part of the Data Protection Directive is aimed at police and the criminal justice sector
GLBA – the Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999	All businesses, regardless of size, that are "significantly engaged" in providing financial products or services to U.S. consumers

[3] Additional data privacy laws are listed in the 2015 International Compendium of Data Privacy Laws published by BakerHostetler

HIPAA – the Health Information Portability and Accountability Act	All U.S. entities and their business associates (BAs) that have access to, process, store or maintain any protected health information
HITECH – the Health Information Technology for Economic and Clinical Health Act	All U.S. entities and their business associates (BAs) that have access to, process, store or maintain any protected health information
ITAR – the International Traffic in Arms Regulations	All entities that manufacture, sell and distribute defense and space-related articles and services on the United States Munitions List
NERC CIP – the North American Electric Reliability Corporation Critical Infrastructure Protection standards	Operators of North America's bulk electric system, also a regulatory reference for many other regions around the world
NIST – National Institute of Standards and Technology Cybersecurity Framework	Any entity that wants to follow a voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure
PCI DSS – Payment Card Industry Data Security Standard	All organizations or merchants, regardless of size or number of transactions, that accept, transmit, process or store cardholder data belonging to various card brands
SOX – the Sarbanes-Oxley Act of 2002	All U.S. publicly-traded companies, along with their wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the U.S.

Table 1: A Partial List of Regulations

Enterprise Security Policy Challenges

In addition to the external regulatory forces, most organizations have their own internal rules to enforce at the networking level. However, there are still some organizations that haven't yet defined an internal security policy. In such cases, they may need help to build and define the policy, which is considered a best practice for improving network security.

In general terms, an enterprise security policy is a living document that states how a company plans to protect its physical and information technology assets. The main challenge is that the policy is typically very complicated; since networks are becoming highly dynamic to serve the highly agile business of today, it's difficult to track all the changes and maintain continuous compliance with the enterprise policy.

An enterprise's security policy typically includes an acceptable use policy. Rules stemming from the acceptable use policy could include which subnets and hosts the company approves (whitelist) or disallows (blacklist) for access via the company network or from inbound traffic. For example, an organization might choose to blacklist employee access to fantasy sports sites, assuming they have no practical business use. On the other hand, it would whitelist IP addresses for web services that play an important role in business operations, such as approved SaaS applications.

Many enterprises today subscribe to threat intelligence services that routinely compile IP addresses of known security threats; for example, command and control servers for botnets and compromised websites. Such lists are updated frequently, and the speedy nature of this task might preclude validating that the new or updated rules don't cause a compliance violation.

Another major challenge is that inter-zone access for east-west traffic must align with compliance requirements to ensure proper segmentation. For example, the NERC CIP Version 5 standard for the energy sector mandates that power grid Cyber Assets grouped into Bulk Electric System (BES) Cyber Systems and categorized by Impact Factor according to their risk categorization on the critical infrastructure. These are be defined by policies and segmentation must be managed centrally across the across the enterprise to reduce the attack surface while maintaining compliance.

And finally, enterprises with legacy technologies face additional challenges for security and compliance. A recent study by Gartner[4] noted that “legacy configuration management tools are not policy-based. They are not always capable of real-time reporting or correlating network issues with device configurations… Network automation is required to meet enterprises' requirements for data center and hybrid cloud agility.”

The Operational Steps for Assuring Compliance in a Complex IT Environment

Despite all the challenges of the complexity of today's IT environment and the mounting number of enterprise policies and regulatory requirements, it's possible to have continuous compliance through good organization, thorough processes and technology automation. First we'll look at the general steps to take, and then we'll look at the essential automation that underpins the entire process.

We've identified six operational steps that are critical to assuring continuous compliance:

1. Define the organizational security policy
2. Capture the existing network topology
3. Define the system architecture and remodel the topology per enterprise policy
4. Identify security gaps and align to the policy
5. Create a well-defined and auditable process for change requests
6. Get ready for audits

Let's have a look at each step and why it is a critical element of continuous compliance.

Step 1: Define the Organizational Security Policy

The organizational security policy is a business-driven construct that defines how the company plans to protect its information and technology assets. The high-level security policy should be defined with all of the following in mind: the external regulatory mandates and industry standards the organization must observe (e.g., PCI DSS, NIST, SOX, HIPAA, NERC CIP, etc.); internal governance requirements (e.g., acceptable use policy); and general best practices that the company observes.

[4] “Effective Network Orchestration Starts by Automating Provisioning”, Simon Richard, 31 August 2015

A company's security policy may include a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

To operationalize this unified security policy, the specific requirements will need to be translated into the technical rules that define what is and isn't allowed for traffic flowing to/through security devices in the various network segments. As an example, a merchant that accepts branded credit cards is regulated by PCI DSS and must establish and control a security perimeter around the segment of the network that collects, processes or stores sensitive cardholder data. No other type of application is permitted to share or have access to this network segment. The organization must then establish rules that control what connections and traffic are permitted into and out of the PCI DSS segment of the network.

Step 2: Capture the Existing Network Topology

Most enterprises networks have undergone considerable changes in the past decade or so. There has been a massive technological shift in topology as organizations embrace virtualization, cloud computing, mobile computing, software-defined infrastructures, and so on. Therefore it's critical to gain visibility into the existing network topology, including all segments and zones, across on-premises, cloud and hybrid networks. Enterprises must have deep insight into their network topology in order to derive the number of security zones they need to manage. This network map must also include all of the business applications, their connectivity and dependencies; and the existing security policies across vendors and platforms. That's a very tall order! All of this information is vital input in order to understand the current security and compliance posture, and ultimately to create repeatable tasks for process automation. The ideal scenario would be to have all of this information in one convenient place—one that is *not* a manual spreadsheet!

Step 3: Define the System Architecture and Remodel the Topology According to Enterprise Policy

The next step is to define the system architecture, based on the security zones dictated by the enterprise policy that will best protect data and applications. Protecting the perimeter is no longer sufficient and internal segmentation is required to segregate sensitive assets from generally accessible zones. Those who oversegment their network, defining a security zone per application for example, face risks and costs of complicated security monitoring and management.

Having an accurate representation of the network topology map can help analyze the network segmentation that is established by legacy and next generation firewalls, and identify what additional segregation is required.

Step 4: Identify Security Gaps and Align to the Policy

At this stage, the unified security policy is the "desired" state of the network and not necessarily the "actual" state of the network. The actual state is the aggregation of the security policies across the different platforms, whether those are security rules and micro-segmentation in physical and virtual firewalls, or security groups in private and public cloud platforms. This is when it's necessary to compare the two, identify any security gaps that exist, and, ideally, take measures to close those gaps and bring the network configuration into full compliance with the defined policy.

Continuing with the PCI DSS example above, the "desired" state is that no other application has access to the network segment that processes the payment application. However, after comparing the model to the actual state, a gap analysis shows that a marketing application also resides on that portion of the network in order to have occasional access to customer data from the payment application. Not only is this a significant violation of PCI DSS, but it also puts the enterprise at risk for a costly data breach. This condition should be flagged for remediation.

Step 5: Create a Well-defined and Auditable Process for Change Requests

Cleaning up the network environment and getting the "actual" state to match the "desired" state of policy is just the beginning. Next the organization needs a process for dealing with requests for network configuration changes. Change requests can occur often because business needs change over time. For example, many companies are adopting methodologies like DevOps where changes to applications are being pushed out very rapidly. It's often the case where application updates require modifications to the network configuration, and these changes need to be made very quickly to keep pace with business. The network team must have a process to respond to requests promptly.

Each configuration change has the potential of violating the security policy and causing a "non-compliant" status that can be detected in an audit and possibly lead to a security breach or other repercussions. When the network is "clean" (i.e., fully compliant with policy), it's important to assess the change requests and the impact they will have and recertify that the network is maintaining its state of continuous compliance.

With the rapid pace of network security changes, recertification of policies, firewall rules and change requests is critical for survival in the compliance jungle. Some regulations, such PCI DSS and the latest NERC CIP Version 5 Cyber Security Standards for the energy sector, actually require regular review and recertification processes/workflows for existing policies as part of demonstrating compliance. In general, recertification makes rule optimization easier, including cleansing, removal of shadowed, unused and overly permissive rule bases. Furthermore, recertification enables full accountability of network security changes. The recertification process includes evaluating the request against the policy to see if the requested configuration change is permitted; in other words, it doesn't cause a policy violation. If it does cause a conflict, the request should be sent to someone with the authority to make a decision to reject the request as submitted, suggest it be modified, or allow it for a designated period of time. If it is allowed, it should be assigned an expiration date to ensure that the non-compliant action isn't left in place permanently.

Furthermore, this change control process needs to include creating documentation of precisely what changes are made, for what business purpose, and at whose request. The documentation needs to include sufficient comments so that auditors can know what happened and why. This documentation is critically important if problems arise and the origins of changes need to be traced.

This repetition of this recertification process makes it ideal for an automated workflow process.

Step 6: Get Ready for Audits

It's not unusual for an organization to align its policies to pass a specific audit, and then go back to its normal way of work after the audit. Not only is this a resource-intensive approach, but it does little to nothing to improve security and to validate the true nature of compliance. The better approach, of course, is to maintain continuous compliance with the overall security policy so that the organization is ready anytime for an audit, regardless of whether it's internal or external. The documented procedures and documentation of change activities from all of the steps above are needed to support the audits. Other ways to demonstrate regulatory compliance include reporting, change audits and history, and recertification with each change.

Your Survival Kit: The Tufin Orchestration Suite™

There's a lot of complexity in the steps listed above, and complexity compounds risk. The only way to survive the process is with Network Security Policy Orchestration. It helps an organization discover when it is at risk, and provides guidance on what to do to mitigate the risk.

The Tufin Orchestration Suite™ delivers the necessary automation across physical, virtual and hybrid environments. Tufin's Unified Security Policy™ (USP) provides the ability to centrally manage all of the organizational security policies in a single place, through a single pane of glass management system. The Orchestration Suite provides visibility into all of the applications on the network and their relationships to each other and to the security devices. The Tufin solution then builds and maintains a dynamic model of the network topology, including all network segments and application connectivity dependencies, regardless of whether they are local to the enterprise's data center, in the cloud or in a hybrid IT environment. An analytics engine thoroughly explores the possibilities of risk and ensures that all future changes in the network are aligned with the centralized policies, and any new violations that might be introduced to the network are alerted on. The Tufin solution identifies gaps in security and alerts on violations of policy so they can be mitigated. And finally, the Tufin Orchestration Suite keeps enterprises ready for audits at any time through an automated audit trail, on-demand reports and compliance documentation.

The Suite is composed of several components that interact with each other as well as with the network infrastructure and the business applications to analyze the risk of changes and then send the changes throughout the infrastructure once approved. The Suite also supports application programming interfaces (APIs) to communicate with other important elements of the computing environment, such as an IT service management system. The architecture is illustrated in Figure 1.

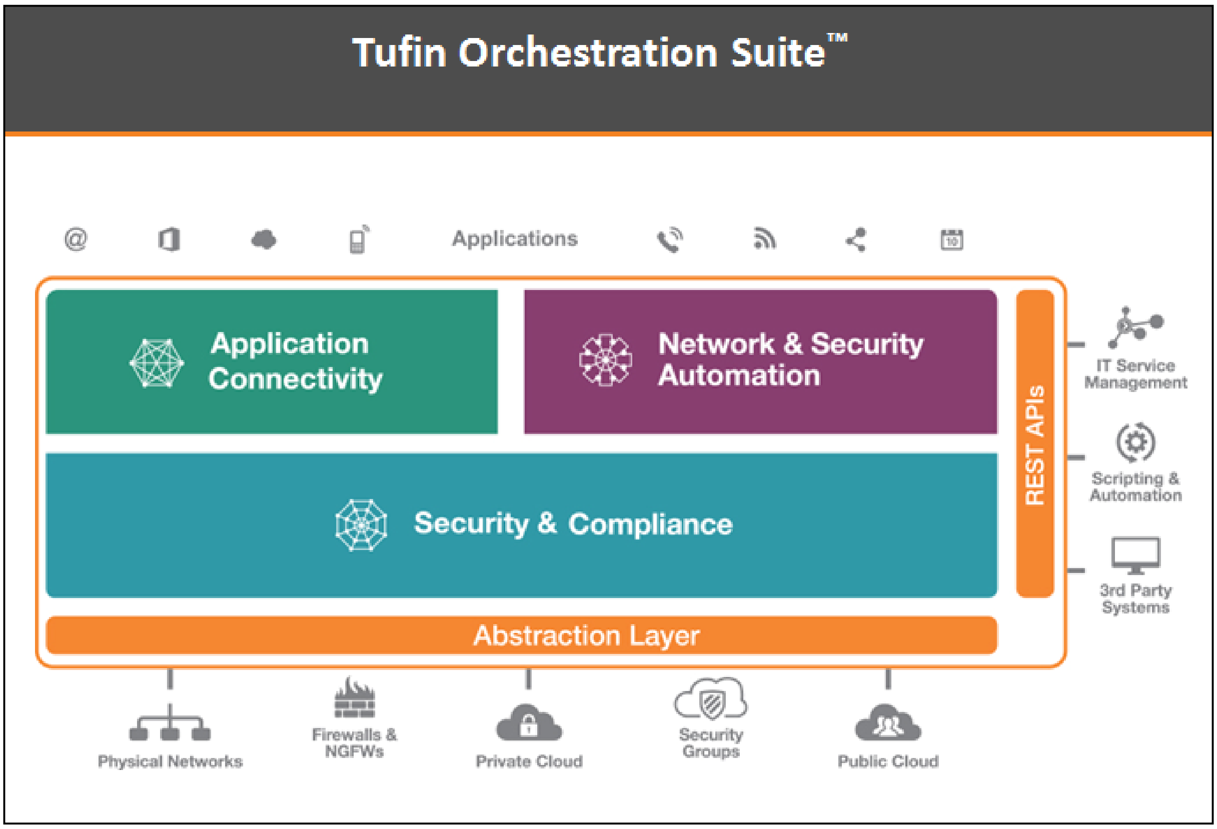


Figure 1: The Architecture of the Tufin Orchestration Suite

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

- The ***Application Connectivity*** component allows an organization to model its business applications and services, defining the network resources they require in order to work. This layer is able to identify and inventory the network resources and make note of which applications the security devices must communicate with.

- The ***Security & Compliance*** component holds the enterprise's Unified Security Policy for the entire IP network. The USP (described in more detail below) defines the desired/required security policies that must be enforced in the organization. These include segmentation policies, best practices policies, regulatory compliance policies, 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 to ensure that these automated changes are not breaking or violating the desired security and overall compliance policies.

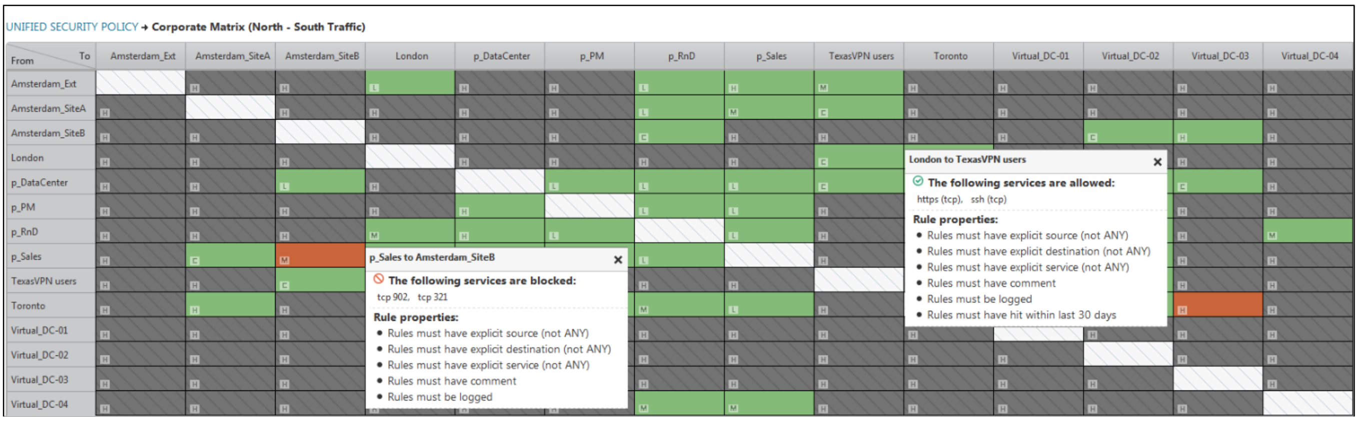
- The ***Abstraction Layer*** component hides the network complexities from the other components. It maps and holds the network topology and interacts with the different networking and security technologies running in the network.

- The ***RESTful APIs*** component enables full programmability to any of the suite's components, allowing easy integration with other enterprise systems and technologies.

It's important to note that all of these components operate across physical and virtual networks, and across cloud-based as well as internal applications and systems.

One of the most important elements of the Tufin solution is the Unified Security Policy, or USP. The USP provides the ability to centrally manage all of the organizational security policies in a single place. The USP automates the complicated process of managing policies, the complex rule bases and a constant influx of change requests for multi-vendor/multi-technology networks. Beginning with the legacy configuration, the USP controls the actual versus desired network segmentation, highlighting existing policy violations so that the enterprise can mitigate the conflicts. Once the network is "clean," alerts on violations before a security change is made can help prevent breaking compliance or exposing the network to unnecessary risk. The USP ensures that all future changes in the network are aligned with the centralized policy and any new violations introduced to the network are alerted on.

The USP gives a simple visual representation of the network segmentation across a multi-vendor array of firewalls, routers and other devices existing across an organization's network. The represented zones can be on a physical, virtual or hybrid network. Figure 2 shows the user interface of the USP, in this case demonstrating the PCI DSS matrix with restricted services. The colored blocks represent the communication permissions between different segments, or zones, of the overall enterprise network. It's possible to tell with a glance what services, if any, are permitted between segments.



UNIFIED SECURITY POLICY → **Corporate Matrix (North - South Traffic)**

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	London	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users	Toronto	Virtual_DC-01	Virtual_DC-02	Virtual_DC-03	Virtual_DC-04
Amsterdam_Ext		H	H	L	H	H	L	H	M	H	H	H	H	H
Amsterdam_SiteA	H		H	H	H	H	L	M	C	H	H	H	H	H
Amsterdam_SiteB	H	H		H	H	H	C	H	H	H	H	C	H	H
London	H	H	H		H	H	H	H	C				H	H
p_DataCenter	H	H	L	H		L	L	L	C				C	H
p_PM	H	H	H	H	H		L	L	H				H	H
p_RnD	H	H	H	M	H	L		L	H				H	M
p_Sales	H	C	M				L		H				H	H
TexasVPN users	H	H	C				H	H					H	H
Toronto	H	H	H				M	L	H				H	H
Virtual_DC-01	H	H	H				H	H	H	H		H	H	H
Virtual_DC-02	H	H	H				H	H	H	H	H		H	H
Virtual_DC-03	H	H	H				H	H	H	H	H	H		H
Virtual_DC-04	H	H	H	H	H	H	M	M	H	H	H	H	H	

p_Sales to Amsterdam_SiteB ×

The following services are blocked:

tcp 902, tcp 321

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged

London to TexasVPN users ×

The following services are allowed:

https (tcp), ssh (tcp)

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days

Figure 2 – The enterprise-wide Unified Security Policy zone matrix

Another significant aspect of the Tufin "survival kit" for compliance is the automated network security change process. Most industry regulations require that security changes adhere to a standard, auditable change process with detailed documentation. Some regulations also require complying with an automated process. The Tufin Orchestration Suite enables defining and enforcing the change process for security changes, or extending the change process that is enforced by the enterprise change-management system. The change process can be automated end-to-end -- through proactive security and compliance analysis, change design and implementation -- to maximize agility and ensure policy control. The Tufin solution also identifies and alerts on changes made outside the change-management process as well as changes that do not align with the approved change request.

Conclusion

Tufin helps enterprises meet the challenges of regulatory and organizational compliance requirements through Network Security Policy Orchestration, enforcing the Unified Security Policy, automation of network configuration and change management. The Tufin solution performs the critical task of identifying applications, their existing connection-dependencies and device configurations. This aids in grouping assets so that policies can be consistently evaluated and applied and continuously monitored for compliance across all enterprise platforms—physical, virtualized and cloud.

Tufin helps organizations focus on continuous compliance and audit readiness with both internal and external requirements. Every network change is automatically documented in an audit trail. There is an automated risk assessment before every change is made. The workflow process requires business approval for changes before they can be made. Once approved, the changes are automatically propagated throughout the appropriate security devices. There is validation of completion of the entire process, which provides evidence of compliance for audits. Moreover, the automated workflow process helps an organization reduce its need for education and training, manual work, and the tedious work of capturing evidence of what is happening.

In summary, the Tufin Orchestration Suite is an essential tool for organizations that need to secure their complex networks and maintain continuous compliance and audit readiness.

About Tufin

Tufin® is the leader in Network Security Policy Orchestration for enterprise cybersecurity. Tufin enables organizations to centrally manage, visualize and control security policies across hybrid cloud and physical network environments. The award-winning Tufin Orchestration Suite™ is a policy-centric solution for automatically analyzing risk, designing, provisioning and auditing network security changes. Tufin reduces the attack surface and minimizes disruptions to critical applications. Its network security automation enables enterprises to implement security changes in minutes instead of days with continuous compliance and increased agility. Tufin serves over 1,700 enterprise customers in industries worldwide, including finance, telecom, energy and utilities, healthcare and pharmaceuticals, retail, education, government, manufacturing and transportation. Tufin's products and technologies are patent-protected in the U.S. and other countries.