tufin

Simplify Network Segmentation Management

Solution Brief

Why Network Segmentation?

Enterprises networks are extremely large and dynamic. The main purpose of the enterprise network is to provide connectivity between applications, data and users to maintain business continuity. In the past, the common method to protect the network was placing a single firewall at the perimeter of the network, thereby isolating the internal IT assets from the external world. As networks became more and more connected and complex, understanding exactly where the perimeter is, became challenging. Furthermore, regulatory compliance requires rule separation between sensitive data (like personal information, or credit card information) and other organizational data.

As a result, network segmentation was initially developed to ease management of large networks and improve network performance. Soon it became obvious that segmentation has great value for network security. According SANS Institute network segmentation is one the top 20 Critical Security Controls for Effective Cyber Defense (source: https://www.sans.org/critical-security-controls/).

The concept of network segmentation is quite simple: Applications and services are classified and grouped into segments (also called zones) by security profile; each segment has a security control at its perimeter. This ensures that even if one network segment is breached, the intrusion is contained and the rest of the network remains secure.

Most enterprise networks today include many segments. The most common method for segmentation is by placing multiple firewalls through the enterprise network. The network and IT security teams need to manage this separation between different segments (like DMZ, datacenter, subnets, branches, PCI zones and so forth), and equally important – the required connectivity and dependencies.

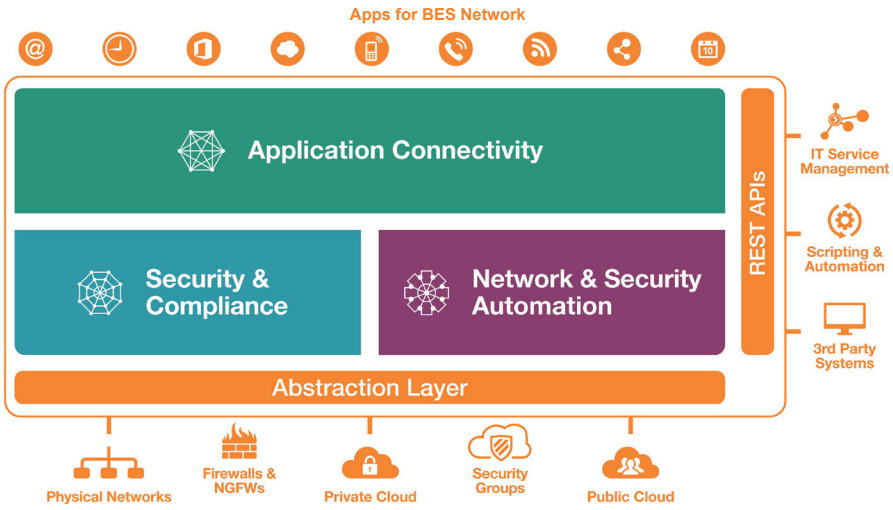
The Challenges

- Have clear visibility across heterogeneous network segments to:
  - Ensure the zone boundaries are well-defined and maintained
  - Enable connected from and to the segment based on business needs
  - Auditability for regulation compliance
  - Identify which security controls are affected for each network change
- Proactively assess network changes to determine in advance if a change will “break” segmentation
- Provide alerts when a change causes a break in segmentation
- Manual and time-consuming processes for managing segmented networks

Benefits to Your Business:

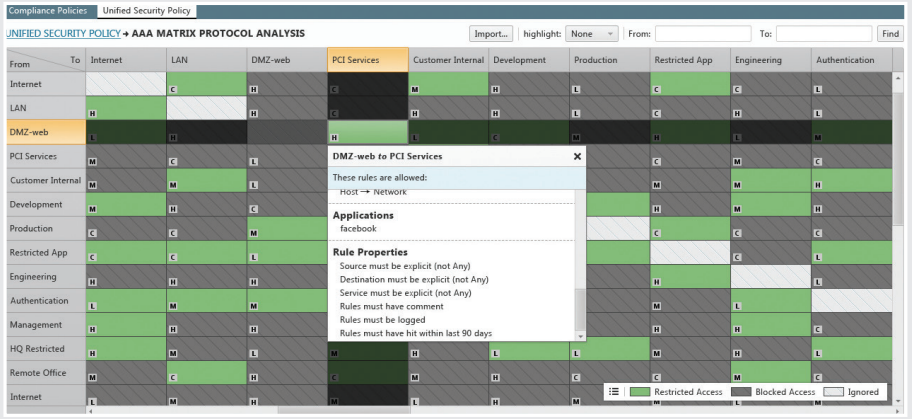
- Reduce attack surface for mitigation of cyber threats
- Manage segmentation via a single console for the entire network environment -- physical firewalls, virtual and cloud platforms
- Proactively analyze risks associated with network changes prior to the actual change
- Implement network changes securely in minutes
- Ensure continuous network compliance and auditability
- Enable easy audit preparation and troubleshooting via automatic audit trail

The Tufin Orchestration Suite™ Solution for Network Segmentation



Tufin's solution for network segmentation enables enterprises to:

- Visualize and manage network segmentation using Tufin Orchestration Suite™
- Streamlined management of the security zone matrix
- Preserve segmentation by
  - Proactively assess network changes to preserve segmentation
  - Automated security control modification
- Single interface to manage the entire network environment (physical firewalls or virtual environments, eg, VMware NSX or cloud security groups)



Tufin's Zone-based Unified Security Policy enables policy optimization, network segmentation and reducing attack surface

Tufin at a Glance

Offices: North America, Europe and Asia-Pacific

Customers: More than 1,600 in over 50 countries

Leading verticals: Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation and auditors

Channel partners: More than 240 worldwide

Technology Partners & Supported Platforms: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Intel Security, Juniper Networks, Microsoft Azure, Openstack, Palo Alto Networks, VMware and more

amazon web services™ · bmcsoftware · BlueCoat · Check Point SOFTWARE TECHNOLOGIES LTD. · Microsoft Azure · CISCO · F5 · FORTINET · intel Security · JUNIPER NETWORKS · openstack · paloalto NETWORKS · servicenow · vmware

tufin

www.tufin.com

SB-10-15