

**SECURITY POLICY MANAGEMENT
USING ANUTA NCX**

**Challenges
Faced by
Security
Teams**

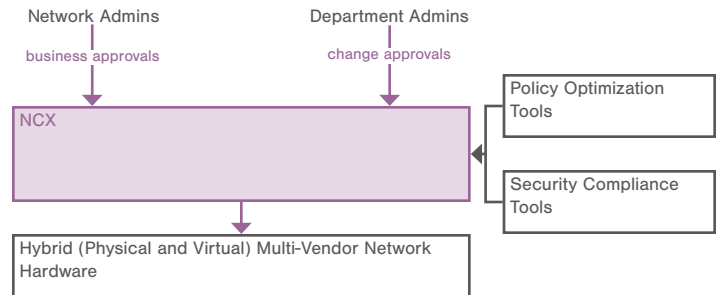
- Network and Security teams work in silos resulting in a disjointed process to deliver end-to-end network services.
- Firewall rule management is inefficient and error prone due to legacy homegrown tools.
- High volume of change requests result in gigantic firewall rules, application-identity mappings, router ACLs

**NCX
Solution**

Anuta NCX provides discovery, configuration management and monitoring capabilities for different vendor firewalls. In addition to delivering end to end network service orchestration, NCX also provides a faster and accurate automation to manage firewall rules. NCX enables organizations to meet today’s huge application demands and stringent security requirements.

NCX Features

- Topology Discovery
- Configuration-based discovery of security zones, VRs and application-identity pairs
- Full CRUD capability
- Per Tenant/per VDC view
- Built-in IPAM and VLAN manager
- Service monitoring
- Audit log and compliance reports
- REST API Integration with security policy automation tools (e.g. Algosec).



NCX Benefits

- | | |
|--|---|
| <p>Simplified firewall rule management reduces operational overhead.</p> | <p>Provides service-level view including Firewall, LB, Routing, Switching, LAN/WAN configuration.</p> |
| <p>End-to-End service chaining ensures application reachability.</p> | <p>Vendor agnostic rule base in the UI, integration with external DB and Policy manager tools.</p> |

Scalability & Performance

NCX has a proven record of managing thousands of firewall rules on hundreds of devices for different use cases such as perimeter security for Public clouds and enterprise private clouds, ACL management in huge carrier networks etc.

Vendor Support

NCX supports firewalls from major vendors including Cisco, Checkpoint, Juniper, Fortinet, Palo Alto and VMWare