Panorama Template and Device Group Migration Plan - PRSCo to New PAN

# Based on Current Configuration Analysis

# Executive Summary

This document outlines the migration strategy from the existing PRSCo Panorama configuration to a new Panorama instance following Palo Alto Networks best practices. The plan preserves the current organizational structure while implementing a more scalable and maintainable architecture.

# Current State Analysis

## Existing Structure Summary

* \*\*31 Location-based templates\*\* (Template\_[Location])
* \*\*14 Device groups\*\* under PRSCo parent
* \*\*2 Template stacks\*\* (PRSCo\_DataCenter, Ensono\_Managed\_s)
* \*\*Mixed naming conventions\*\* requiring standardization
* \*\*Multi-tenant VSYS deployment\*\* with Ensono integration

## Identified Gaps vs Best Practices

1. \*\*Template Organization\*\*: Location-specific templates lack modular base configurations

2. \*\*Naming Inconsistencies\*\*: Mixed formats (e.g., Template\_Indy vs Template\_Indianapolis IN)

3. \*\*Limited Template Stacks\*\*: Only 2 stacks for 31 templates

4. \*\*Flat Device Group Structure\*\*: Most groups directly under PRSCo

5. \*\*No Clear Separation\*\*: Network, security, and system configs mixed in templates

# Proposed New Architecture

## 1. Enhanced Template Structure

Panorama Templates

├── Base Templates (New - Shared Configuration)

│ ├── PRSCo-System-Base-v1

│ │ ├── DNS/NTP settings (from DatacenterBase)

│ │ ├── Management profiles

│ │ ├── Log forwarding (ITG Logging)

│ │ └── Authentication (PRSCo AD)

│ │

│ ├── PRSCo-Network-Base-v1

│ │ ├── Network profiles

│ │ ├── QoS profiles

│ │ └── Zone protection profiles

│ │

│ └── PRSCo-Security-Base-v1

│ ├── Security profiles

│ ├── Vulnerability protection

│ ├── Anti-spyware profiles

│ └── URL filtering profiles

│

├── Regional Templates (New - Regional Specifics)

│ ├── US-Common-v1

│ │ ├── US-specific routing

│ │ ├── Regional DNS servers

│ │ └── Compliance settings

│ │

│ ├── Canada-Common-v1

│ │ └── Canadian compliance requirements

│ │

│ └── Mexico-Common-v1

│ └── Mexican regulatory requirements

│

├── Function Templates (Preserve existing concepts)

│ ├── DataCenter-Function-v1 (from DatacenterBase)

│ ├── Remote-Branch-Function-v1

│ ├── VPN-Function-v1 (from VPN templates)

│ ├── Internet-Edge-Function-v1

│ └── DMZ-Function-v1

│

└── Site-Specific Templates (Migrate from existing)

├── US Sites

│ ├── Site-Warrenville-v1 (from Template\_Warrenville)

│ ├── Site-Indianapolis-Main-v1 (from Template\_Indy)

│ ├── Site-Indianapolis-Airtech-v1

│ └── [... other US sites ...]

│

├── Canada Sites

│ └── Site-Newmarket-ON-v1 (from Template\_Newmarket ON)

│

└── Mexico Sites

├── Site-Tlalnepantla-v1

├── Site-San-Juan-Rio-v1

├── Site-Galeana-v1

└── Site-VPN-Galeana-v1

## 2. Improved Template Stack Design

Template Stacks (Hierarchical combinations)

├── DataCenter Stacks

│ ├── DC-PRSCo-Primary-Stack

│ │ ├── PRSCo-System-Base-v1

│ │ ├── PRSCo-Network-Base-v1

│ │ ├── PRSCo-Security-Base-v1

│ │ ├── US-Common-v1

│ │ ├── DataCenter-Function-v1

│ │ └── PRSCo\_Admin\_Roles

│ │

│ └── DC-Ensono-Managed-Stack

│ ├── PRSCo-System-Base-v1

│ ├── PRSCo-Network-Base-v1

│ ├── PRSCo-Security-Base-v1

│ ├── US-Common-v1

│ ├── DataCenter-Function-v1

│ └── Ensono\_Admin\_Roles\_t

│

├── US Branch Stacks

│ ├── Branch-Indianapolis-Stack

│ │ ├── PRSCo-System-Base-v1

│ │ ├── PRSCo-Network-Base-v1

│ │ ├── PRSCo-Security-Base-v1

│ │ ├── US-Common-v1

│ │ ├── Remote-Branch-Function-v1

│ │ └── Site-Indianapolis-Main-v1

│ │

│ └── [... stacks for each US location ...]

│

├── International Branch Stacks

│ ├── Branch-Canada-Newmarket-Stack

│ │ ├── PRSCo-System-Base-v1

│ │ ├── PRSCo-Network-Base-v1

│ │ ├── PRSCo-Security-Base-v1

│ │ ├── Canada-Common-v1

│ │ ├── Remote-Branch-Function-v1

│ │ └── Site-Newmarket-ON-v1

│ │

│ └── Branch-Mexico-[Location]-Stack

│ └── [Similar structure with Mexico-Common-v1]

│

└── Special Purpose Stacks

├── VPN-Gateway-Stack

├── Internet-Edge-Stack

└── Lab-Testing-Stack

## 3. Enhanced Device Group Hierarchy

Device Groups

├── Shared (Global Objects)

│ ├── Address Objects

│ ├── Service Objects

│ ├── Application Groups

│ ├── Tags

│ └── EDLs

│

├── PRSCo-Global-PreRules

│ ├── Critical-Block-Rules

│ ├── Management-Access

│ └── Compliance-Mandated

│

├── PRSCo (Root - Preserved)

│ ├── DataCenters

│ │ ├── PRSCo-Managed-DC

│ │ │ ├── Identity-Processing (existing)

│ │ │ ├── Utility-Firewall-Cluster (existing)

│ │ │ └── User-Firewall-Cluster (existing)

│ │ │

│ │ └── Ensono-Managed-DC

│ │ └── Ensono-DG (existing)

│ │

│ ├── Remote-Sites

│ │ ├── US-Branches

│ │ │ ├── US-Central

│ │ │ │ ├── Indianapolis-Sites

│ │ │ │ │ ├── Indy-Main

│ │ │ │ │ ├── Indy-Airtech

│ │ │ │ │ └── Indy-Decatur

│ │ │ │ ├── Illinois-Sites

│ │ │ │ └── Missouri-Sites

│ │ │ │

│ │ │ ├── US-East

│ │ │ │ ├── Connecticut-Sites

│ │ │ │ ├── Massachusetts-Sites

│ │ │ │ └── NewYork-Sites

│ │ │ │

│ │ │ └── US-South

│ │ │ ├── Texas-Sites

│ │ │ └── Virginia-Sites

│ │ │

│ │ ├── Canada-Branches

│ │ │ └── Ontario-Sites

│ │ │

│ │ └── Mexico-Branches

│ │ ├── MexicoCity-Region

│ │ └── Central-Mexico

│ │

│ ├── Security-Functions

│ │ ├── VSYS-Groups

│ │ │ ├── ECOM-VSYS (existing)

│ │ │ ├── SSL-VSYS (existing)

│ │ │ ├── PCI-VSYS (existing)

│ │ │ ├── Peer-VSYS (existing)

│ │ │ └── Interco-VSYS (existing)

│ │ │

│ │ └── Special-Purpose

│ │ ├── Remote-DMZ-Firewalls (existing)

│ │ ├── LSC-Internet-Firewall (existing)

│ │ ├── LSC-VPN-Firewall (existing)

│ │ └── LAB-Firewall (existing)

│ │

│ └── Cloud-Infrastructure (New)

│ ├── AWS-Firewalls

│ ├── Azure-Firewalls

│ └── GCP-Firewalls

│

└── PRSCo-Global-PostRules

├── Default-Deny-All

└── Logging-Rules

# Migration Timeline - September 2025

## Week 1 (Sep 1-7): Foundation & Analysis

**Day 1-2: Environment Setup**

* ☐ Deploy new Panorama instance
* ☐ Configure authentication (PRSCo AD integration)
* ☐ Set up ITG Logging profiles
* ☐ Import certificates (Digicert\_CA, Panorama\_Mgmt\_Cert)

**Day 3-4: Create Base Templates**

* ☐ Create PRSCo-System-Base-v1

- Import DNS/NTP from DatacenterBase

- Configure log forwarding to ITG Alienvault

- Set up management profiles

* ☐ Create PRSCo-Network-Base-v1

- Define standard zones

- Configure network profiles

* ☐ Create PRSCo-Security-Base-v1

- Import existing security profiles

- Configure threat prevention

**Day 5-7: Regional Templates**

* ☐ Create US-Common-v1
* ☐ Create Canada-Common-v1
* ☐ Create Mexico-Common-v1

## Week 2 (Sep 8-14): Function Templates & Migration Prep

**Day 8-10: Function Templates**

* ☐ Create DataCenter-Function-v1 (based on DatacenterBase)
* ☐ Create Remote-Branch-Function-v1
* ☐ Create VPN-Function-v1
* ☐ Create Internet-Edge-Function-v1
* ☐ Create DMZ-Function-v1

**Day 11-14: Site Template Migration Planning**

* ☐ Map existing 31 templates to new structure
* ☐ Document site-specific configurations
* ☐ Create migration matrix
* ☐ Standardize naming conventions

## Week 3 (Sep 15-21): Site Templates & Stacks

**Day 15-17: Priority Site Templates**

* ☐ Migrate Warrenville template
* ☐ Migrate Indianapolis templates (consolidate 3 variants)
* ☐ Migrate Plainfield templates (consolidate variants)
* ☐ Create first 10 template stacks

**Day 18-21: Remaining Site Templates**

* ☐ Migrate remaining US site templates
* ☐ Migrate international templates
* ☐ Create all template stacks
* ☐ Validate inheritance chains

## Week 4 (Sep 22-30): Device Groups & Testing

**Day 22-24: Device Group Creation**

* ☐ Create complete hierarchy
* ☐ Import existing security policies
* ☐ Configure policy rules in appropriate groups
* ☐ Set up shared objects

**Day 25-27: Lab Testing**

* ☐ Deploy test firewalls
* ☐ Validate template inheritance
* ☐ Test policy precedence
* ☐ Verify logging and monitoring

**Day 28-30: Documentation & Signoff**

* ☐ Complete migration documentation
* ☐ Create runbooks
* ☐ Stakeholder review
* ☐ Obtain migration approval

# Migration Timeline - October 2025

## Week 1 (Oct 1-7): Data Center Migration

**Day 1-3: PRSCo Managed DC**

* ☐ Migrate Identity Processing firewalls
* ☐ Migrate Utility Firewall Cluster
* ☐ Migrate User Firewall Cluster
* ☐ Validate all DC services

**Day 4-5: Ensono Managed DC**

* ☐ Coordinate with Ensono team
* ☐ Migrate Ensono-DG devices
* ☐ Update Ensono admin roles
* ☐ Test Ensono monitoring

**Day 6-7: VSYS Migration**

* ☐ Migrate ECOM VSYS
* ☐ Migrate SSL, PCI, Peer, Interco VSYS
* ☐ Validate VSYS isolation

## Week 2 (Oct 8-14): Special Purpose & Pilot Sites

**Day 8-10: Special Purpose Firewalls**

* ☐ Migrate Remote DMZ Firewalls
* ☐ Migrate LSC Internet/VPN Firewalls
* ☐ Migrate LAB Firewall

**Day 11-14: Pilot Branch Migration**

* ☐ Select pilots: Warrenville, Indianapolis Main, Newmarket, Tlalnepantla
* ☐ Execute pilot migrations
* ☐ 48-hour monitoring period
* ☐ Document lessons learned

## Week 3 (Oct 15-21): US Branch Migration

**Day 15-17: Central Region**

* ☐ Indianapolis sites (3 locations)
* ☐ Crawfordsville sites (2 locations)
* ☐ Plainfield sites (3 locations)
* ☐ Other Indiana sites

**Day 18-19: East Region**

* ☐ North Chelmsford
* ☐ Norwalk CT
* ☐ Garden City NY

**Day 20-21: Central/South Region**

* ☐ Missouri sites (4 locations)
* ☐ Wisconsin sites (3 locations)
* ☐ Texas and Virginia sites

## Week 4 (Oct 22-28): International Migration

**Day 22-23: Canada Migration**

* ☐ Newmarket ON
* ☐ Coordinate with Canadian team
* ☐ Validate compliance requirements

**Day 24-26: Mexico Migration**

* ☐ Tlalnepantla
* ☐ San Juan Rio
* ☐ Galeana (including VPN)
* ☐ Coordinate with Mexico team

**Day 27-28: Final Validation**

* ☐ Network-wide connectivity tests
* ☐ Application validation
* ☐ Performance benchmarking
* ☐ Security audit

## Week 5 (Oct 29-31): Cutover & Closure

**Day 29: Legacy Decommission Prep**

* ☐ Final backup of old Panorama
* ☐ Document any remaining issues
* ☐ Prepare decommission plan

**Day 30: Go-Live Declaration**

* ☐ Official cutover to new Panorama
* ☐ Update all documentation
* ☐ Communication to all stakeholders

**Day 31: Project Closure**

* ☐ Lessons learned session
* ☐ Knowledge transfer completion
* ☐ Handover to operations
* ☐ Archive project artifacts

# Risk Mitigation Specific to Current Environment

## High-Risk Items

1. \*\*VSYS Migration Complexity\*\*: Multiple virtual systems with different tags

2. \*\*Ensono Integration\*\*: Requires coordination with external team

3. \*\*31 Unique Templates\*\*: Risk of configuration drift during migration

4. \*\*Multi-Country Deployment\*\*: Time zone and compliance considerations

## Mitigation Strategies

1. \*\*Phased VSYS Migration\*\*: Migrate one VSYS at a time with validation

2. \*\*Ensono Coordination\*\*: Dedicated liaison and testing window

3. \*\*Template Validation\*\*: Automated comparison tools for before/after

4. \*\*Regional Teams\*\*: Local support during migration windows

# Success Metrics

1. \*\*Zero Downtime\*\*: No unplanned outages during migration

2. \*\*Policy Parity\*\*: 100% of security policies successfully migrated

3. \*\*Performance\*\*: No degradation in throughput or latency

4. \*\*Compliance\*\*: All regulatory requirements maintained

5. \*\*Documentation\*\*: Complete runbooks for future operations

---

\*\*Document Version\*\*: 2.0

\*\*Created\*\*: September 2025

\*\*Last Updated\*\*: September 2025

\*\*Based on\*\*: Current PRSCo Panorama Configuration Analysis