Detailed SD-WAN Implementation Steps

Phase 1: Implement New PAN VM (POC for Production)

**Lead: LSC | Timeline: Weeks 1-2**

1.1 Infrastructure Requirements

VM Specifications:

• Panorama VM: 32GB RAM, 16 vCPUs, 2TB storage

• CPU: Intel x86-64 architecture

• Network: Minimum 4 network interfaces

• Hypervisor: VMware vSphere 7.0+ or AWS/Azure/GCP

1.2 Licensing Requirements

• Panorama VM license

• Device management licenses (minimum 25 devices)

• SD-WAN plugin license

• Support license (Premium recommended)

1.3 Pre-deployment Tasks

1. Contact Palo Alto Networks (LSC - In Progress)

• Request POC licenses

• Schedule deployment assistance

• Obtain latest Panorama VM image

• Confirm SD-WAN plugin compatibility

2. Infrastructure Preparation

• Allocate VM resources

• Configure network connectivity

• Set up DNS entries

• Configure NTP servers

• Prepare backup storage

1.4 Deployment Steps

1. Deploy Panorama VM

Initial configuration:

• Management IP: [To be assigned]

• Default gateway: [To be configured]

• DNS servers: [Corporate DNS]

• NTP servers: [Corporate NTP]

2. Initial Setup

• Access Panorama web interface

• Complete initial setup wizard

• Apply licenses

• Configure administrator accounts

• Enable RADIUS/LDAP authentication

3. Install SD-WAN Plugin

• Download SD-WAN plugin 3.2.x

• Install via Panorama > Plugins

• Restart management services

• Verify plugin installation

Phase 2: Create Device Templates and Groups

**Lead: LSC | Support: Ensono | Timeline: Weeks 2-4**

2.1 Template Hierarchy Structure

Panorama

├── Template Stack: Global-Base-Stack

│ ├── Template: Global-Network-Base

│ ├── Template: Global-Security-Base

│ └── Template: Global-System-Base

├── Template Stack: SDWAN-Hub-Stack

│ ├── Template: SDWAN-Hub-Network

│ ├── Template: SDWAN-Hub-Zones

│ └── Template: SDWAN-Hub-Interfaces

└── Template Stack: SDWAN-Branch-Stack

├── Template: SDWAN-Branch-Network

├── Template: SDWAN-Branch-Zones

└── Template: SDWAN-Branch-Interfaces

2.2 Device Group Hierarchy

Device Groups

├── Shared-Objects

│ ├── Address Objects

│ ├── Service Objects

│ └── Tags

├── Global-PreRules

│ └── Security Policies

├── SDWAN-Hubs

│ ├── Hub-Site-A

│ └── Hub-Site-B

└── SDWAN-Branches

├── Region-1-Branches

├── Region-2-Branches

└── Region-3-Branches

2.3 Global Base Templates (LSC)

2.3.1 Global-Network-Base Template

Management Settings:

• Management interface configuration

• Service routes

• DNS/NTP configuration

System Settings:

• Device certificates

• Authentication profiles

• Log forwarding profiles

• SNMP configuration

2.3.2 Global-Security-Base Template

Security Profiles:

• Antivirus profiles

• Anti-spyware profiles

• Vulnerability protection

• URL filtering

• File blocking

• WildFire analysis

Security Rules Framework:

• Default deny rules

• Management access rules

• Logging rules

2.4 SD-WAN Specific Templates (Ensono to assist)

2.4.1 SDWAN-Hub-Network Template

Zone Configuration Example:

*<\!-- Zone Configuration -->*

<zone>

<entry name="SDWAN-HUB">

<network>

<layer3>

<member>ethernet1/1</member>

<member>ethernet1/2</member>

</layer3>

</network>

</entry>

</zone>

2.4.2 SDWAN-Branch-Network Template

• WAN interface configurations

• LAN interface configurations

• SD-WAN link settings

• Path monitoring

2.5 Variable Implementation

Site Variables CSV Example:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| site-name | wan1-ip | wan2-ip | lan-subnet | bgp-as | location |
| BRANCH-001 | 203.0.113.10 | 198.51.100.10 | 192.168.1.0/24 | 65001 | New York |
| BRANCH-002 | 203.0.113.20 | 198.51.100.20 | 192.168.2.0/24 | 65002 | Chicago |

Phase 3: Testing and Migration Plan

**Lead: LSC | Support: Ensono | Timeline: Weeks 5-7**

3.1 Lab Testing Environment

3.1.1 Lab Setup Requirements

Hardware:

• 2x PA-VM-50 (Lab firewalls)

• 1x Test workstation

• Network simulator for WAN conditions

Network Design:

Lab-Hub-FW --- WAN-Simulator --- Lab-Branch-FW

| |

Hub-LAN-Test Branch-LAN-Test

3.1.2 Test Cases

1. Basic Connectivity Tests

• Management access

• Template push validation

• Commit operations

• High availability failover

2. SD-WAN Functionality Tests

• VPN tunnel establishment

• Path selection

• Application-based routing

• Link failover

• QoS validation

3. Security Policy Tests

• Inter-zone traffic

• Internet breakout

• Application identification

• Threat prevention

3.2 Migration Plan for Existing Palos

3.2.1 Pre-Migration Assessment

1. Inventory Current Devices

Export current configurations:

scp export configuration from running-config.xml

2. Document Current State

• Interface assignments

• Routing tables

• Security policies

• NAT rules

• VPN configurations

3. Identify Migration Groups

• Group 1: Non-critical branches (Week 8)

• Group 2: Standard branches (Week 9-10)

• Group 3: Critical sites (Week 11)

• Group 4: Hub sites (Week 12)

3.2.2 Migration Methodology

1. Per-Device Migration Steps

Step 1: Backup current config

request system backup config

Step 2: Export config to Panorama

request panorama export device-config

Step 3: Clean local configuration

delete vsys vsys1

set vsys vsys1

commit

Step 4: Connect to new Panorama

set deviceconfig system panorama-server <NEW-PANORAMA-IP>

commit

2. Validation Checklist

☐ Device appears in new Panorama

☐ Templates successfully pushed

☐ SD-WAN plugin installed

☐ Policies deployed

☐ Connectivity verified

3.3 Rollback Procedures

1. Immediate Rollback (<1 hour)

• Restore from running-config backup

• Revert Panorama connection

2. Extended Rollback (1-24 hours)

• Maintain parallel operations

• Gradual traffic migration

• Policy synchronization

Phase 4: Configure SD-WAN Hub and Spoke

**Lead: Ensono | Support: LSC | Timeline: Weeks 8-12**

4.1 Hub Configuration Details

4.1.1 Primary Hub Setup

Hub Name: SDWAN-HUB-PRIMARY

Location: Primary Data Center

Device: PA-5220 or PA-VM-500

Interfaces:

• ethernet1/1: ISP-1 (Public)

• ethernet1/2: ISP-2 (Public)

• ethernet1/3: MPLS

• ethernet1/4: LAN-CORE

SD-WAN Profile:

• Type: hub

• Mesh-Group: HUB-MESH

• Advertisement: Local subnets, Default route

4.1.2 Hub SD-WAN Configuration

XML Configuration Example:

<sdwan>

<devices>

<entry name="SDWAN-HUB-PRIMARY">

<hub>

<advertise-default-route>yes</advertise-default-route>

<max-branches>100</max-branches>

<mesh-group>HUB-MESH</mesh-group>

</hub>

</entry>

</devices>

</sdwan>

4.2 Branch Configuration Details

4.2.1 Branch Profile Template

Branch Type: Standard-Branch

Devices: PA-850 or PA-VM-50

Interfaces:

• ethernet1/1: ISP-1 (DHCP/Static)

• ethernet1/2: ISP-2 (DHCP/Static) [Optional]

• ethernet1/3: LAN

SD-WAN Settings:

• Type: branch

• Hub-Connection: SDWAN-HUB-PRIMARY

• Backup-Hub: SDWAN-HUB-SECONDARY

4.2.2 Path Selection Policies

Path Quality Profiles:

|  |  |  |  |
| --- | --- | --- | --- |
| Profile | Latency (ms) | Jitter (ms) | Packet Loss (%) |
| VOICE-QUALITY | 150 | 30 | 1 |
| DATA-QUALITY | 300 | 50 | 2 |

4.3 Traffic Distribution Profiles

4.3.1 Application-Based Routing

Business-Critical Applications:

• Voice Applications: SIP, MS Teams Audio

• Path Quality Profile: VOICE-QUALITY

• Priority: High

4.3.2 QoS Implementation

Traffic Classes:

• Real-time (Voice): 20% guaranteed

• Business-critical: 40% guaranteed

• Default: 30% guaranteed

• Bulk: 10% best effort

4.4 Monitoring and Optimization

4.4.1 Monitoring Setup

• Enable SD-WAN monitoring

• Configure SNMP traps

• Set up Syslog forwarding

• Create custom reports

4.4.2 Performance Baselines

• Document latency targets

• Set jitter thresholds

• Define packet loss limits

• Establish bandwidth utilization goals

Implementation Schedule Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Week | Phase | Activities | Owner |
| 1-2 | PAN VM Setup | Deploy Panorama, obtain licenses | LSC |
| 2-4 | Templates | Create device templates and groups | LSC/Ensono |
| 5-7 | Testing | Lab validation and migration planning | LSC/Ensono |
| 8 | Hub Deploy | Configure primary hub | Ensono/LSC |
| 9-10 | Branch Wave 1 | Deploy 30% of branches | Ensono |
| 11 | Branch Wave 2 | Deploy 60% of branches | Ensono |
| 12 | Branch Wave 3 | Deploy remaining branches | Ensono |
| 13 | Optimization | Performance tuning | Ensono |
| 14 | Documentation | Finalize runbooks | LSC/Ensono |

Success Metrics

Technical KPIs

• Tunnel uptime: >99.95%

• Failover time: <3 seconds

• Application performance: Meeting SLA

• Security events: <5% increase

Business KPIs

• User satisfaction: >90%

• Reduced WAN costs: 20-30%

• Improved application response: 25%

• Simplified management: 50% reduction in tasks