Seqrite
Endpoint Protection

DNS-Based Hybrid Communication Architecture and Deployment Guide

Patch Server | Dec 2025

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Protection is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Introduction

This guide describes the architecture and communication flow of the on-premises patch infrastructure for the Seqrite EPP Patch Server, configured and managed using DNS. It provides an overview of how internal and remote devices interact with the patch server, the role of network components (switches, load balancer/firewall, DNS), and the overall infrastructure setup.

Problem Statement

The Seqrite EPP Patch Server supports configuration using either IP address or fully qualified domain name (FQDN).

If configured using **only a public IP address**:

- LAN endpoints connect via the public network.
- Remote endpoints connect via the internet.
- LAN traffic hairpins through the WAN, resulting in latency, bandwidth waste, and firewall dependency.

Solution: DNS-Based Configuration.

Configure the Patch Server using FQDN and implement split-horizon DNS:

- **Internal DNS record** → Local IP
- **Public DNS record** → Public IP / Load balancer / Firewall NAT
- **Split-horizon DNS** → Automatic routing
    - LAN devices resolve to the internal IP.
    - Remote devices resolve to the public IP.

This ensures seamless hybrid connectivity for all endpoints, regardless of network location.

System Overview

Purpose: Why DNS-Based Configuration Matters

DNS-based configuration allows internal and roaming devices to reach the Patch Server using a single FQDN. Devices automatically route via the internal IP when inside the network and the

public IP when outside. This eliminates static IP dependency and ensures seamless patch delivery.

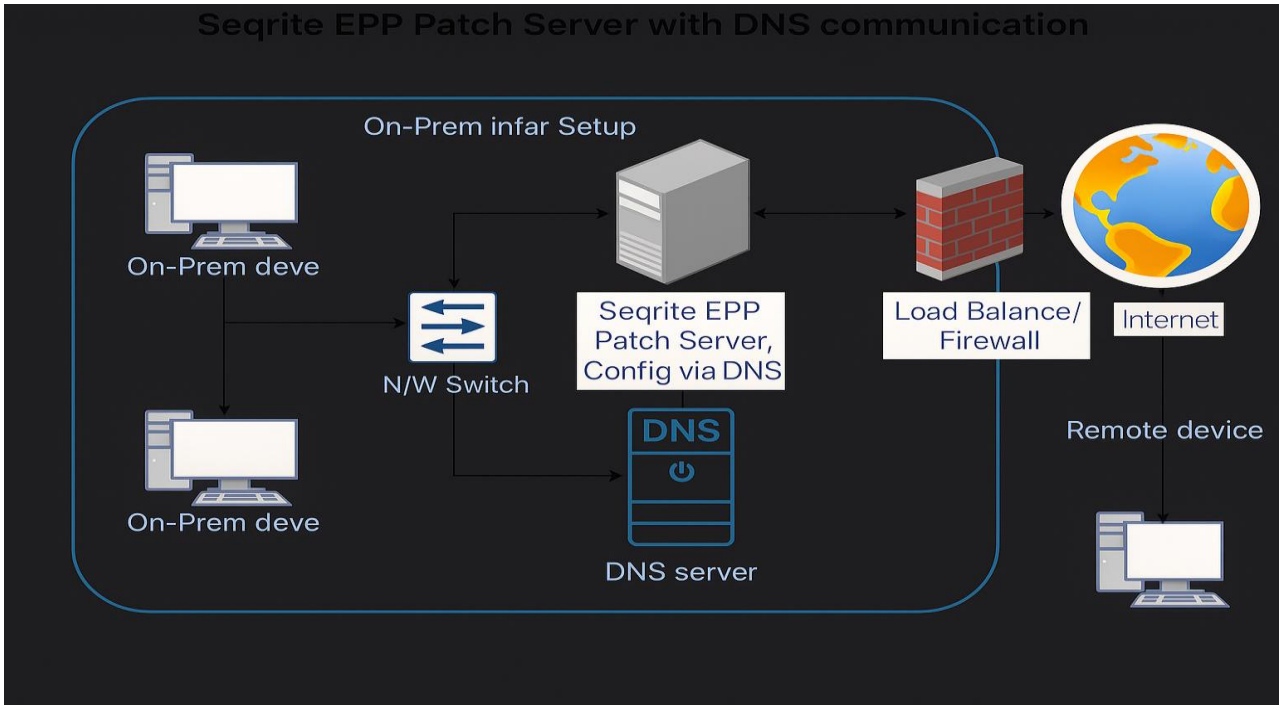
Benefits and Best Practices

- Simplifies routing for internal and external devices.
- Reduces manual configuration and static IP issues.
- Ensures consistent patch delivery.
- **Best practice**: Always use one FQDN and configure split DNS for internal/public resolution.

High- Level Flow

- LAN clients → Internal DNS → Internal IP → Patch Server
- Roaming clients → Public DNS → Public IP → Firewall/Load balancer → Patch Server
- Patch Server → Serves patches, metadata, and filters based on policies

Architecture Diagram



Communication Flow

Internal Devices (On Premises)

1. Device resolves FQDN via internal DNS, returning the internal IP.
2. Device connects through the local network switch to the Patch Server.
3. Device retrieves patches, updates, status, or configuration.

Remote Devices

1. Device connects via the internet and resolves FQDN via public DNS, returning the public IP or load balancer IP.
2. Connection reaches the firewall or load balancer.
3. Firewall/load balancer NATs traffic to the internal IP.
4. Patch Server handles the request as for LAN devices.

DNS Interactions

- Clients rely on DNS, not static IPs, to locate the Patch Server.
- DNS records must be updated to reflect infrastructure changes.

Prerequisites

Technical Requirements

- Internal DNS server (AD, Windows DNS, BIND, etc.)
- Public DNS management access
- Firewall or load balancer supporting NAT
- Installed and reachable Seqrite EPP Patch Server

Information Required

- Internal Patch Server IP (for example, 10.x.x.x)
- Public IP or load balancer IP
- Patch Server FQDN (for example, patch.company.com)

Required Ports

- DNS port for resolution
- Firewall/load balancer rules allowing traffic in both LAN and public directions

Bandwidth Requirements

- Patch distribution may consume 4–5 Mbps, depending on patch size.
- WAN links should be sized based on the number of roaming users.
- Internal LAN can handle distribution without WAN usage when DNS is correctly configured.

Configuration Procedures

DNS Configuration

- **Internal DNS record**: Create or update an A or CNAME record for the Patch Server FQDN pointing to the internal IP.
- **Public DNS record**: Create an A or CNAME record for the same FQDN pointing to the public IP behind the load balancer/firewall.
- **Split-horizon DNS**: Ensure local VLAN clients resolve the FQDN to the internal IP, while external clients resolve to the public IP.

Validation

- From a local VLAN machine: nslookup patchserver.company.com → returns internal IP.
- From a remote location: nslookup patchserver.company.com → returns public IP.

Network Switch and VLAN Configuration (LAN)

- Verify that internal switches and VLANs allow endpoints to communicate directly with the Patch Server internal IP and DNS server.
- Ensure routing/firewall rules do not force local traffic through the internet.
- Validate connectivity by pinging/resolving the FQDN from a local VLAN device.

Firewall/Load Balancer Setup (Roaming Clients)

- Forward traffic from the firewall/load balancer to the Patch Server internal IP.
- Configure health checks to ensure Patch Server availability.
- Apply TLS/SSL and firewall rules according to security policy.

Patch Server Configuration

- Configure the Patch Server with FQDN, not IP.
- Ensure connections are accepted from LAN subnets and external NAT IPs.
- Validate filter policies (device type, OS version, location).
- Test connectivity from both local VLAN endpoints and roaming clients.
- Ensure patch reporting, logging, and backup/restore mechanisms are in place.

Conclusion

DNS-based configuration ensures that the Seqrite EPP Patch Server reliably serves both LAN and roaming devices without requiring separate configurations or IP switching. This architecture improves efficiency, security, and manageability for large and distributed environments.