sase.cloud

SASE + SSE Deploy 101

The complete deployment guide.

What's inside:

- 20-point pre-deployment audit checklist
- 5 deployment phases with step-by-step checkpoints
- TLS bypass list — 30+ domains to whitelist on day 1
- DLP regex patterns — copy-paste ready for PCI, PII, secrets
- ZTNA posture templates — three-tier policy framework
- Troubleshooting playbook for every phase
- Success metrics and ROI proof points for leadership

BEFORE YOU START

Pre-deployment audit

Complete every item before touching SASE configuration. Skipping items here causes delays, outages, and rollbacks later.

IDENTITY & ACCESS

- [ ] IdP configured (Okta / Azure AD / Ping) — SAML 2.0 or OIDC endpoints ready
- [ ] MFA enforced for all users, not just admins
- [ ] User groups mapped to application access tiers (admin / standard / contractor)
- [ ] Service accounts inventoried — these cannot use ZTNA agents
- [ ] Break-glass / emergency access accounts documented and tested

NETWORK INFRASTRUCTURE

- [ ] DNS architecture documented — split-horizon zones, internal domains (.corp, .local)
- [ ] Current WAN topology mapped — MPLS circuits, broadband, LTE backup per site
- [ ] MPLS contract renewal dates logged — never migrate mid-contract
- [ ] Branch internet bandwidth tested (up and down) at each site
- [ ] Existing firewall rules exported — decide which move to cloud, which stay local

ENDPOINT READINESS

- [ ] MDM/UEM coverage confirmed — percentage of managed vs unmanaged devices
- [ ] Root CA distribution method tested (GPO for Windows, MDM profile for macOS/iOS)
- [ ] OS distribution documented — Windows 10/11 split, macOS versions, Linux distros
- [ ] Existing VPN client uninstall plan — conflicts with ZTNA agents are common

APPLICATION INVENTORY

- [ ] Top 50 SaaS applications identified by usage volume
- [ ] Internal web apps cataloged — URLs, ports, authentication methods
- [ ] Thick-client / non-HTTP applications listed — these need VPN fallback
- [ ] Certificate-pinned applications identified — these MUST bypass TLS decryption

ORGANIZATIONAL READINESS

- [ ] Executive sponsor identified and briefed on phased timeline
- [ ] Helpdesk team trained on agent install, TLS bypass requests, ZTNA access issues
- [ ] User communication drafted — what changes, why, and who to call
- [ ] Rollback criteria defined per phase — what metrics trigger a rollback

PHASE 1 • HOURS TO 1 DAY

DNS-layer security

The fastest, lowest-risk first step. Redirect DNS to your SASE vendor's resolver to block malicious domains. No agent, no TLS decryption, no user-visible changes.

Deploy checklist

- [ ] Redirect recursive DNS to SASE vendor resolver (conditional forwarders for split-horizon)
- [ ] Enable default block categories: malware, phishing, C2, cryptomining, newly registered domains
- [ ] Allowlist business-critical domains that might be miscategorized
- [ ] Enable DNS query logging for baseline traffic visibility
- [ ] Configure DNS sinkholing for blocked domains (return safe page, not connection error)
- [ ] Test split-horizon resolution — internal .corp / .local zones must still resolve internally
- [ ] Verify DNS-over-HTTPS (DoH) in browsers is either blocked or routed through SASE

CHECKPOINT — Do not proceed until all pass

- [ ] All client DNS queries route through SASE resolver (verify with nslookup/dig from 3+ devices)
- [ ] Internal domain resolution works correctly (test 5 internal hostnames)
- [ ] Block categories active — test with known malware domain (e.g., vendor test URL)
- [ ] Zero user-reported access issues for 24 hours

Troubleshooting

Internal domains not resolving
Add conditional forwarding rules for all internal zones (.corp, .local, .internal). Check that the SASE resolver forwards to your internal DNS server, not public DNS.

Browser bypassing SASE DNS via DoH
Push browser policy via GPO/MDM to disable DoH, or configure DoH to use your SASE vendor's DoH endpoint if supported.

False positives blocking legitimate domains
Check the vendor's categorization database. Submit recategorization requests. Add to allowlist immediately while request processes — don't block users waiting for reclassification.

DNS latency increased
Verify users hit the nearest SASE PoP. Check anycast routing. If latency >50ms, investigate peering between user's ISP and SASE vendor.

Success metrics

Malicious domains blocked / day — 0 (no visibility before)
Target: Track and report monthly — this number sells the project to leadership
DNS resolution latency (p95) — Measure ISP resolver first
Target: <50ms — SASE DNS should match or beat your ISP
User-reported breakage tickets — N/A
Target: <5 in the first week
DNS query visibility coverage — 0%
Target: 100% of managed devices

PHASE 2 • 1 TO 3 WEEKS

SWG + TLS inspection

Deploy the Secure Web Gateway with TLS decryption to inspect encrypted web traffic. This is where you get URL filtering, inline malware scanning, and real visibility into what's happening on the wire.

Deploy checklist

- [ ] Deploy SASE agent to pilot group (50-100 users) via MDM or self-service portal
- [ ] Distribute custom root CA certificate to all managed endpoints (GPO / MDM profile)
- [ ] Apply TLS bypass list (see reference below) BEFORE enabling decryption
- [ ] Enable SWG in monitor-only mode — log all traffic, block nothing for 1-2 weeks
- [ ] Review monitor-only logs: identify false positives, missing bypass rules, broken apps
- [ ] Enable URL filtering policies: block high-risk categories, warn on uncategorized
- [ ] Enable inline malware scanning and file type controls (block executables from unknown sources)
- [ ] Switch from monitor-only to enforce mode for pilot group
- [ ] Expand to all users in waves (dept by dept) over 1-2 weeks
- [ ] Establish a shared Slack/Teams channel for users to report broken sites

CHECKPOINT — Do not proceed until all pass

- [ ] Root CA deployed to 100% of managed endpoints (verify with cert store check)
- [ ] TLS bypass list applied — test certificate-pinned apps from the list below
- [ ] Monitor-only period complete — false positives identified and bypass rules added
- [ ] Pilot group running in enforce mode for 5+ days with <3 daily bypass requests

TLS decryption bypass list

These apps use certificate pinning or mutual TLS. Bypass them BEFORE enabling decryption.

OS & Updates: *.apple.com | *.windowsupdate.com | *.googleapis.com/android | ocsp.*.com | crl.*.com
Financial: Banking portals (cert-pinned) | *.plaid.com | *.stripe.com | *.braintree-api.com | *.adyen.com
Healthcare: EHR portals (Epic, Cerner — mutual TLS) | Insurance claim portals | Telehealth platforms
Dev / DevOps: *.github.com | *.gitlab.com | *.docker.io | registry.npmjs.org | *.pypi.org
Comms: *.teams.microsoft.com (calls) | *.zoom.us | *.webex.com | *.slack.com
Security tools: *.crowdstrike.com | *.sentinelone.net | *.carbonblack.com | Your SASE vendor agent domains

Troubleshooting

Website shows certificate error after TLS decryption enabled
Root CA not installed on the device. Verify cert store. On macOS, the profile must be both installed AND trusted (two separate steps). On Linux, update ca-certificates bundle.

App completely non-functional (not just cert error)
Likely certificate pinning. Add to TLS bypass list immediately. Common offenders: banking apps, Teams calls, EDR agents.

Noticeable page load slowdown
Check if user is hitting the nearest PoP (run traceroute to SASE proxy). Verify single-pass inspection is enabled, not sequential chaining. Target: <100ms added latency at p95.

Agent causing high CPU on endpoint
Check for conflicts with existing VPN client or proxy PAC file. Only one proxy should be active. Uninstall legacy proxy/VPN before deploying SASE agent.

Success metrics

Web traffic inspected (TLS decrypted) — 0%
Target: 80%+ (never 100% — bypasses are expected)
Malware blocked inline — Whatever your previous proxy caught
Target: Track monthly — this metric justifies the entire project

TLS bypass list as % of traffic — N/A
Target: <15% — if higher, your bypass list is too broad
Page load latency added (p95) — Measure baseline first
Target: <100ms added — imperceptible to users
User-reported site breakage — N/A
Target: Trending to <2/day within 2 weeks

PHASE 3 • 1 TO 3 MONTHS

VPN to ZTNA migration

Replace VPN with Zero Trust Network Access. Per-app access, identity-verified, posture-checked. Start with low-risk apps to build user confidence, then migrate business-critical systems. Run VPN in parallel — never cut over cold.

Deploy checklist

- [ ] Inventory all internal applications accessed via VPN — categorize by risk and user count
- [ ] Deploy ZTNA connectors in data center and cloud VPCs (outbound-only, no inbound ports)
- [ ] Test connector connectivity from 2+ PoPs — verify tunnel stability over 24 hours
- [ ] Configure posture policies per application tier (see posture templates below)
- [ ] Pilot with 3-5 low-risk internal web apps and 50-100 friendly users
- [ ] Monitor ZTNA access logs for failed connections, posture failures, latency issues
- [ ] Migrate business-critical apps (ERP, CRM, source code) — one app at a time
- [ ] Enable continuous posture verification (ZTNA 2.0) if vendor supports it
- [ ] Run VPN + ZTNA in parallel for 4-8 weeks per application
- [ ] Disable VPN access per-app as ZTNA reaches 90%+ adoption for that app
- [ ] Document legacy exceptions — thick-client apps that genuinely require VPN

CHECKPOINT — Do not proceed until all pass

- [ ] ZTNA connectors healthy and reachable from all PoPs (verify from 3+ geographic locations)
- [ ] Posture policies enforcing correctly — test with a non-compliant device (should be denied)
- [ ] Pilot users accessing all 3-5 apps via ZTNA with zero VPN fallback for 7+ days
- [ ] Connection time measured and faster than VPN (use this data in comms to users)

ZTNA posture templates

Three tiers mapped to application sensitivity. Start with Standard for most apps.

STRICT — Production & admin (AWS console, database, SSH)
OS patched within 14 days | EDR running + healthy | Disk encryption on
MFA within last 60 min (step-up) | MDM compliant | Screen lock < 5 min

STANDARD — Business apps (Salesforce, Jira, email, ERP)
OS patched within 30 days | EDR running | Disk encryption on
MFA within last 8 hours | MDM registered

BASIC — Low-risk (intranet, wiki, directory)
Authenticated via IdP | MFA within 24 hours
OS not end-of-life | No active malware alerts

Troubleshooting

User passes auth but ZTNA connector unreachable
Connector is down or tunnel between connector and PoP is broken. Check connector status in dashboard. Verify outbound ports (typically 443) are open from connector network. Restart connector service.

App loads but specific features broken (e.g., file upload, WebSocket)
ZTNA proxy may not support all protocols natively. Check if app uses WebSockets, chunked transfer, or long-polling. Some vendors need explicit protocol support enabled. Fall back to VPN for this specific app if needed.

Posture check failing for compliant devices
Check clock sync (posture timestamps are sensitive). Verify EDR agent version meets minimum. On macOS, MDM profile must be approved in System Settings > Privacy. Check that posture signals are reaching the ZTNA broker (agent logs).

Contractors/BYOD cannot access via agentless ZTNA
Verify clientless access is configured for the app. Test in incognito browser. Check IdP federation — contractor IdP must be trusted. Session timeout may be too aggressive for browser-based access.

Success metrics

VPN concurrent sessions — Current peak VPN users
Target: Trending to zero (except documented legacy exceptions)
ZTNA connection time vs VPN — Measure VPN connect time
Target: 2-5x faster — use this in executive reporting
Applications migrated to ZTNA — 0%
Target: 100% of web apps within 3 months; 80% of all apps within 6
Lateral movement attack surface — VPN users could reach N subnets
Target: Users can only reach M specific apps — show the delta

VPN hardware/licensing cost eliminated — Current VPN concentrator + licensing cost
Target: Track dollar savings quarterly

PHASE 4 • 2 TO 4 MONTHS

CASB + DLP

Enable Cloud Access Security Broker for SaaS visibility and Data Loss Prevention for content inspection. Start with shadow IT discovery, then layer in controls. DLP false positives destroy user trust — start narrow, expand slowly.

Deploy checklist

- [ ] Run inline shadow IT discovery for 2-4 weeks — identify all SaaS in use
- [ ] Categorize SaaS into sanctioned / tolerated / unsanctioned tiers
- [ ] Connect API-based CASB to sanctioned SaaS (M365, Google Workspace, Salesforce)
- [ ] Enable CASB inline controls: block uploads to unsanctioned cloud storage
- [ ] Deploy DLP in alert-only mode with 3 high-confidence patterns (see below)
- [ ] Review DLP alerts daily for 2 weeks — tune patterns, add exclusions
- [ ] Switch DLP from alert-only to block for validated patterns
- [ ] Enable SSPM (SaaS Security Posture Management) scans for misconfigurations
- [ ] Set up automated weekly DLP incident report to security team
- [ ] Establish DLP exception request process for business users

CHECKPOINT — Do not proceed until all pass

- [ ] Shadow IT discovery complete — top 20 SaaS by usage documented and categorized
- [ ] API CASB connected to all sanctioned SaaS with OAuth consent from IT admin
- [ ] DLP alert-only running for 2+ weeks with >80% true positive rate
- [ ] Business users have clear process to request DLP exceptions

DLP starter patterns

High-confidence, low-false-positive patterns. Copy-paste into your DLP engine.

Credit cards (PCI-DSS)

```
\b(?:4[0-9]{12}(?:[0-9]{3})?|5[1-5][0-9]{14}|3[47][0-9]{13})\b
```

Visa, MC, Amex. Pair with Luhn checksum.

US Social Security Numbers

```
\b(?!000|666|9\d{2})\d{3}-(?!00)\d{2}-(?!0000)\d{4}\b
```

XXX-XX-XXXX with invalid range exclusion.

API keys & secrets

```
(?:api[_-]?key|api[_-]?secret|bearer)\s*[:=]\s*['"]?[A-Za-z0-9_\-]{20,}
```

Catches API keys in code, config, and chat.

AWS access keys

```
(?:AKIA|ASIA)[A-Z0-9]{16}
```

IAM key IDs. Very high confidence.

Private keys (PEM)

```
-----BEGIN (?:RSA |EC )?PRIVATE KEY-----
```

Always block. Never alert-only.

Bulk email exfiltration

```
Trigger when >50 email addresses in a single file upload
```

Block CSV/DB dumps, not individual emails.

Troubleshooting

DLP blocking legitimate business documents
Pattern too broad. Review the matched content — add proximity rules (require keyword near the pattern) or increase minimum match count. Switch pattern back to alert-only, fix, then re-enable block.

Shadow IT discovery showing 500+ apps
This is normal. Don't try to block everything. Focus on the top 20 by usage and the top 10 by risk score. Tolerate the long tail unless it involves data storage or file sharing.

API CASB connection failing to SaaS tenant
OAuth consent may have expired or been revoked by SaaS admin. Re-authorize the connection. Ensure CASB app has correct API permissions (many require Global Admin for initial setup).

Users circumventing CASB via personal devices
Personal devices bypass inline CASB if they don't have the agent. Enforce: managed devices only for sanctioned SaaS (Conditional Access in Azure AD), or deploy agentless reverse proxy for browser-based access.

Success metrics

Shadow IT applications discovered — Unknown
Target: 200-500+ is typical — report the top 20 to leadership (this number shocks CISOs)
DLP incidents / week (true positive) — 0
Target: >80% true positive rate before enabling block mode
Unsanctioned cloud storage uploads — Unknown
Target: Track before/after — show reduction to leadership quarterly
SaaS misconfigurations found (SSPM) — Unknown
Target: Remediate all critical and high findings within 30 days
DLP exception requests / month — N/A
Target: <10 — if higher, patterns need tuning

PHASE 5 • 3 TO 6 MONTHS

SD-WAN rollout

Deploy SD-WAN at branch locations. Replace or augment MPLS with application-aware routing, automated failover, and direct internet breakout for SaaS. Run alongside MPLS — never cut MPLS before SD-WAN is proven at each site.

Deploy checklist

- [ ] Audit current MPLS contracts — renewal dates, bandwidth, SLA terms, early termination costs
- [ ] Select 3-5 pilot branches including at least one remote / low-bandwidth site
- [ ] Ship SD-WAN edge appliances to pilot sites — pre-stage configs for zero-touch provisioning
- [ ] Deploy dual-transport at each site: broadband + LTE/5G backup (or MPLS + broadband)
- [ ] Configure application-aware routing: direct-to-internet for SaaS, backhaul for internal apps
- [ ] Set per-application SLA thresholds: latency, jitter, packet loss with automatic path failover
- [ ] Enable QoS policies for real-time apps: voice, video, and collaboration tools
- [ ] Monitor pilot sites for 30 days — track SLA adherence, failover events, user experience
- [ ] Expand to remaining branches in waves (5-10 sites per wave)
- [ ] Begin MPLS reduction at sites where SD-WAN has proven 30+ days of stable operation
- [ ] Negotiate MPLS contract downgrades or terminations — document cost savings

CHECKPOINT — Do not proceed until all pass

- [ ] All pilot sites dual-homed with SD-WAN + existing transport active
- [ ] Application-aware routing verified — SaaS going direct, internal traffic backhauled
- [ ] Failover tested at each pilot site — simulate primary link failure, verify <1 second switchover
- [ ] 30 days of monitoring data showing SLA compliance for critical applications
- [ ] No user-reported application performance degradation vs. MPLS baseline

Troubleshooting

Voice/video quality degraded after SD-WAN deployment
QoS policies not applied or not prioritizing real-time traffic. Enable packet duplication or Forward Error Correction (FEC) for voice/video. Verify jitter buffer settings. Check that SD-WAN is not routing real-time traffic over high-latency backup link.

Zero-touch provisioning fails at remote branch
Branch internet may be too unreliable for initial bootstrap. Pre-stage the appliance in your office (configure and test), then ship. Alternatively, use LTE for initial provisioning, then switch to primary link.

SD-WAN tunnel flapping (going up and down repeatedly)
Usually caused by marginal broadband quality. Check link quality metrics — packet loss >1% or jitter >30ms on primary link will cause flapping. Adjust SLA thresholds or upgrade link quality. Enable dead-peer detection tuning.

Application performance worse than MPLS
Check path selection — the SD-WAN may be routing over a suboptimal path. Verify application identification is working (DPI engine needs to correctly classify the app). Run path trace to compare MPLS vs. SD-WAN latency for that specific app.

Success metrics

MPLS cost reduction — Current MPLS spend
Target: Track circuit-by-circuit. 40-60% savings is typical over 12 months.
Application SLA adherence — MPLS baseline
Target: 99.5%+ for critical apps. Measure per-branch, report monthly.
Mean time to recover from WAN failure — Hours (MPLS carrier SLA)
Target: Seconds (SD-WAN auto-failover) — this metric sells to the CFO
SaaS direct internet breakout — 0% (all backhauled)
Target: 100% of SaaS traffic goes direct — zero backhaul to data center
Branches fully migrated — 0
Target: Track weekly. Report to leadership with timeline projection.

EXECUTIVE SUMMARY

ROI proof points for leadership

Present these metrics quarterly. Capture baselines BEFORE deployment — if you don't measure before, you can't prove improvement after. Every metric below has been used successfully to justify SASE investment at the board level.

SECURITY POSTURE IMPROVEMENT

Malicious domains blocked / month — 0 (no DNS-layer visibility)
Target: Hundreds to thousands — proves immediate threat reduction

Web-borne malware blocked inline — Endpoint AV catches only
Target: Show delta — SASE catches threats before they reach the endpoint

Lateral movement attack surface — Users accessed N subnets via VPN
Target: Users access M specific apps via ZTNA — quantify the reduction

Shadow IT SaaS applications discovered — Unknown
Target: 200-500 apps. The number alone justifies CASB investment.

DLP incidents caught (data exfiltration attempts) — 0 (no visibility)
Target: Track weekly. Each prevented incident has quantifiable risk reduction.

COST REDUCTION

MPLS circuit cost savings — Annual MPLS spend
Target: 40-60% reduction over 12-18 months

VPN hardware/licensing eliminated — VPN concentrator + licensing
Target: Full elimination once ZTNA migration completes

Security tool consolidation — Point products: SWG + CASB + FW + DLP
Target: Single SASE license replaces 3-5 point products

Helpdesk ticket volume for remote access — VPN-related tickets / month
Target: 50-70% reduction after ZTNA — users stop calling about VPN issues

USER EXPERIENCE

Remote access connection time — VPN: 5-15 seconds
Target: ZTNA: <1 second — users notice and appreciate the improvement

SaaS application latency (p95) — Backhauled: 150-300ms
Target: Direct breakout: 30-80ms — show before/after to leadership

Helpdesk satisfaction scores — Before SASE baseline
Target: Track quarterly. Remote access complaints should drop significantly.

How to present to leadership:

- Lead with the threat numbers (malware blocked, domains blocked) — security wins budget.
- Show the cost savings second — MPLS reduction, VPN elimination, tool consolidation.
- End with user experience — faster connections, fewer helpdesk tickets, happier employees.
- Always compare to baselines. "We blocked 4,200 malicious domains last month" is good. "We went from zero visibility to blocking 4,200 malicious domains" is better.

sase.cloud

Independent SASE & SSE knowledge
for people who deploy it.

sase.cloud/cheatsheet Full interactive version
sase.cloud/components Component deep dives (ZTNA, SWG, CASB, FWaaS, DLP, DEM)
sase.cloud/vendors Vendor reviews (Cisco, Fortinet, Palo Alto, Check Point)

No vendor affiliation. No sponsorships. Built from deployment experience.
Questions or feedback: hello@sase.cloud