Ultimate VDI Guide for K-12 Schools

Larson Carter
larson@carter.tech

April 17, 2025

Abstract

In response to growing remote-access demands—exacerbated by public health challenges, constrained VPN licenses, and diverse user devices—this guide presents a turnkey solution tailored for K-12 environments. Authored by Larson Carter, it details deploying Apache Guacamole 1.5.x on Ubuntu 24.04LTS, integrating robust Active Directory authentication, and securing desktop sessions behind HAProxy. You will learn how to design VLAN segmentation, obtain and automate TLS certificates, right-size both gateway VMs and host hardware for varied workloads, automate maintenance and renewals, implement monitoring and compliance measures, and customize the UI to match your district's branding. By following these steps, non-technical staff can rapidly provision a scalable, secure remote desktop service—no VPN client required.

Contents

1 Introduction

This guide provides a comprehensive, step-by-step walkthrough to deploy a browser-based remote desktop infrastructure tailored for K-12 schools. Administrators and IT staff will learn how to:

- Establish a hardened Ubuntu 24.04 LTS gateway hosting Apache Guacamole and HAProxy.
- Configure Active Directory integration for single sign-on and group-based permissions.
- Obtain and automate renewal of TLS certificates via Let's Encrypt and Cloudflare.
- Architect network segmentation with dedicated VLANs and static IP assignments.
- Size gateway VMs and host hardware to meet diverse application demands.
- Automate routine maintenance tasks and implement comprehensive monitoring.
- Ensure licensing compliance, secure operations, and audit-ready session recording.
- Customize the Guacamole UI to reflect your district's branding.

By the end of this document, your school will have a reliable, scalable, and user-friendly remote desktop solution—no VPN client required.

2 Problem Statement and Goals

2.1 Problem Statement

Remote instruction demands have led to:

- Overburdened state VPN services with limited concurrent licenses.
- Challenges for users on low-bandwidth or restricted devices.
- High support overhead for non-technical staff configuring VPN clients.

2.2 Goals

- Provide zero-install, browser-based RDP access.
- Offload desktop sessions to centrally managed servers.
- Integrate seamlessly with Active Directory for secure access.
- Simplify user workflows: "log in and launch" classroom applications.
- Scale from small pilots to thousands of concurrent sessions.

3 Assumptions and Prerequisites

- A dedicated Ubuntu 24.04 LTS gateway (2 CPU cores, 6 GB RAM, 50 GB disk per 25 users).
- Active Directory domain controllers reachable from gateway.
- Cloudflare-managed public DNS zone and internal DNS infrastructure.
- VLAN-capable switches with DHCP scopes configured for management, user, and RDP networks.
- Firewall/router capable of port-forwarding HTTPS only.
- Virtualization platform (e.g., VMware, Hyper-V) for hosting Windows VMs.

4 Network Segmentation and DHCP

4.1 Segmentation Strategy

Isolate remote desktop traffic on a dedicated **RDP VLAN (e.g., VLAN 200)** to ensure consistent performance and security.

4.2 DHCP Configuration

- Create a DHCP scope bound to VLAN 200 for Windows VM addresses.
- Reserve static IPs for infrastructure servers (AD DCs, gateway).
- Set default lease time to 8 hours for lab environments.

4.3 Static IP Assignment

Assign a static management IP to the Guacamole/HAProxy gateway:

- **Manual:** edit `/etc/netplan/01-netcfg.yaml` to set IP (e.g., 10.50.0.10).
- **DHCP reservation:** bind MAC address to IP in DHCP server.

5 DNS, TLS, and NAT Configuration

5.1 Internal DNS

- Create an A record for `guac.school.local` → gateway IP.
- Ensure replication across AD-integrated DNS servers.

5.2 Public DNS and Cloudflare

- Add public record `rdp.school.edu` with orange-cloud proxy.
- Enable DNSSEC and WAF features.

5.3 TLS Certificate via Let's Encrypt

1. Install Certbot and Cloudflare plugin.
2. Store Cloudflare API key in `/etc/letsencrypt/cloudflare.ini` (600 permissions).
3. Run:
   ```
   certbot certonly --dns-cloudflare
   --dns-cloudflare-credentials /etc/letsencrypt/cloudflare.ini
   -d rdp.school.edu
   ```
4. Schedule automatic renewals (see Section 16).

5.4 Firewall/NAT Rules

- Forward only TCP 443 from the Internet to the gateway.
- Block all other inbound traffic.
- Allow established sessions to return.

6 VM and Host Sizing

6.1 Gateway VM Sizing

Concurrent Users	CPU Cores	RAM (GB)
1–100	2	6
101–400	3	10
401–1200	6	24
1201–3000	8	28
>3000	Scale accordingly	Scale accordingly

Table 1: Recommended gateway VM sizing by concurrent sessions

6.2 Host Hardware Sizing

Specifications are per machine (no user count references):

- **Basic Gradebook Host:** 2-core CPU, 4 GB RAM, 100 GB SSD.
- **Media Editing Host:** 4-core CPU, 12 GB RAM, 250 GB SSD, GPU passthrough capable.
- **Virtual Lab Host:** 8-core CPU, 16 GB RAM, 500 GB SSD, GPU passthrough capable.

7 System Update and Required Packages

7.1 System Update

```
sudo apt update && sudo apt upgrade -y
```

7.2 Install Base Packages

```
sudo apt install -y git ufw nginx haproxy certbot \
  python3-certbot-dns-cloudflare
```

8 Firewall Configuration (UFW)

```
sudo ufw allow 22/tcp    # SSH
sudo ufw allow 80/tcp    # HTTP (ACME)
sudo ufw allow 443/tcp   # HTTPS
sudo ufw allow 3389/tcp  # RDP via HAProxy
sudo ufw enable
```

9 Installing Easy-Guacamole-Installer

```
git clone https://github.com/itiligent/Easy-Guacamole-Installer.git
cd Easy-Guacamole-Installer
chmod +x 1-setup.sh
./1-setup.sh
```

Follow prompts for hostname, MySQL, LDAP/AD, and Nginx proxy setup.

10 Active Directory Integration

Edit `/etc/guacamole/guacamole.properties`:

```
ldap-hostname: dc1.school.local,dc2.school.local
ldap-port: 389
ldap-username-attribute: sAMAccountName
ldap-encryption-method: none
ldap-search-bind-dn: cn=guacbind,ou=ServiceAccounts,dc=school,dc=local
ldap-search-bind-password: $GUAC_PASSWORD
ldap-config-base-dn: dc=school,dc=local
ldap-user-base-dn: ou=Staff,dc=school,dc=local
ldap-user-search-filter: (objectClass=user)(!(objectCategory=computer))
ldap-max-search-results: 500
mysql-auto-create-accounts: true
```

Additionally, ensure your Organizational Unit (OU) is added to the LDAP groups that have permission to each connection in Guacamole's settings. Restart services:

```
systemctl restart guacd guacamole nginx haproxy
```

11 Installing and Configuring HAProxy

11.1 Install HAProxy

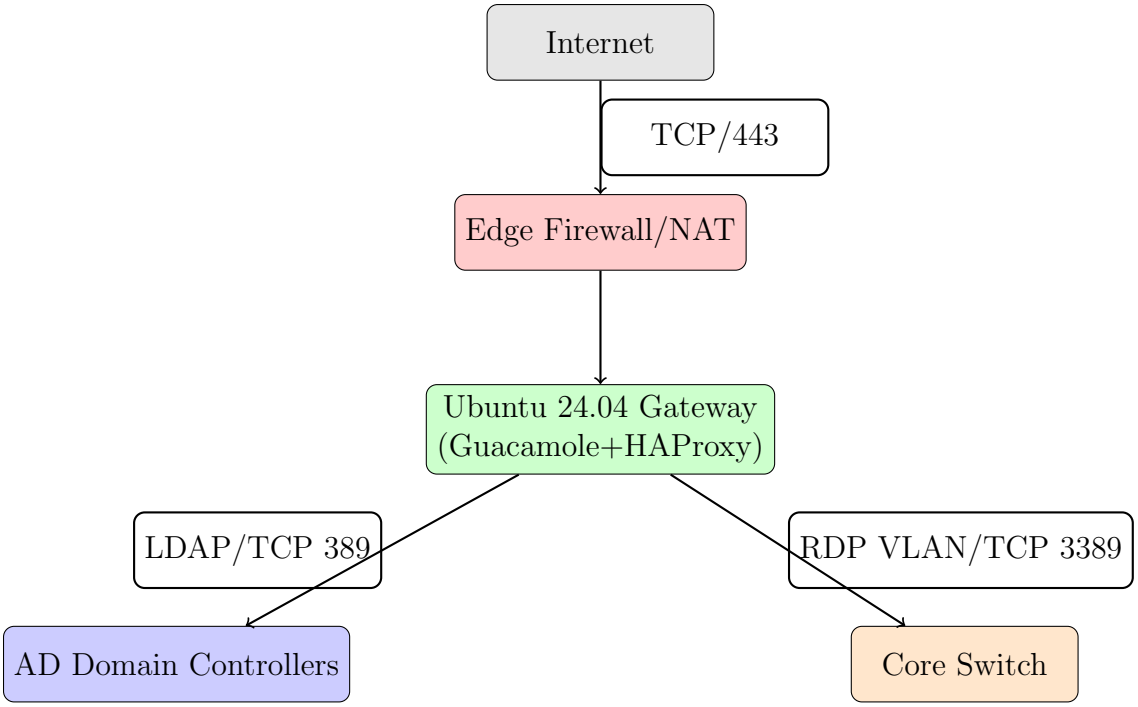
```
sudo apt install -y haproxy
```

11.2 HAProxy Configuration

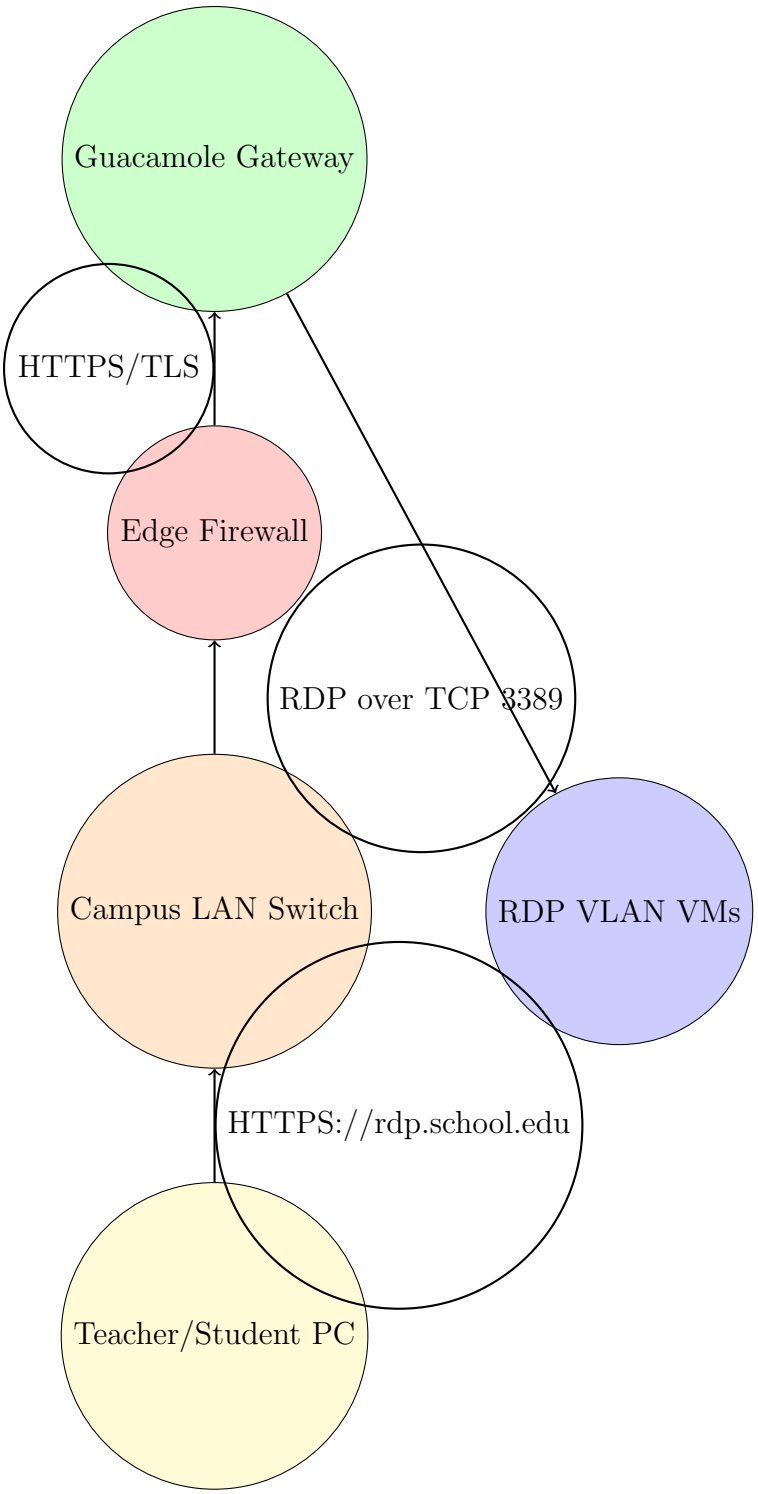
Edit `/etc/haproxy/haproxy.cfg`:

```
# Global settings
global
    log /dev/log local0
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    user haproxy
    group haproxy
    daemon
    maxconn 4096
    ssl-server-verify required

defaults
    log global
    mode tcp
    option dontlognull
    retries 3
    timeout connect 5s
    timeout client 50s
    timeout server 50s

# Admin stats
listen stats
    bind :9000 mode http
    stats enable
    stats uri /stats
    stats auth admin:$tr0ngP@ss

# RDP backend pool
listen RDP
    bind 0.0.0.0:3389
    balance leastconn
    mode tcp
    server VM0 10.50.0.100:3389 check
    server VM1 10.50.0.101:3389 check
    # Add more servers as needed
```

12 School Network Topology



13 End-User Network Topology



14 Adding Connections and Testing

1. Log into the Guacamole admin portal at `https://guac.school.local` as `guacadmin` and immediately change the default password to your secure choice.
2. Navigate to `Settings` → `Connections` and click `New Connection`. Configure:
   - **Name:** e.g., "Gradebook-VM" or "Photoshop-Lab".
   - **Protocol:** RDP.
   - **Parameters:**
     - Remote host: IP of Gateway VM (e.g., 127.0.0.1).
     - Port: 3389.
     - Security mode: "Negotiation" or TLS if configured.
     - Username passthrough: use `${GUAC_USERNAME}` to inherit AD user.
     - Password passthrough: use `${GUAC_PASSWORD}` to inherit AD user.
3. Ensure your AD Organizational Unit (OU) is included in the Guacamole groups that have permission to this connection.
4. Click `Save`, then test connection by launching as an AD user to verify group-based access.

15 Viewing HAProxy Pool Status

The HAProxy stats page (`http://<gateway-IP>:9000/stats`) displays:

- **Frontend/Backend Names**
- **Sessions/sec (sps)**
- **Active Connections**
- **Server Health (UP/DOWN)**
- **In/Out Throughput (bytes)**
- **Check Status and Last Response Time**

Alternatively:

```
echo "show stat" | socat stdio /run/haproxy/admin.sock
```

16 Automated Certificate Renewal

16.1 Systemd Timer

```
sudo systemctl enable certbot-renew.timer
# post-hook to reload services on renewal
mkdir -p /etc/letsencrypt/renewal-hooks/post
cat << 'EOF' > /etc/letsencrypt/renewal-hooks/post/reload.sh
#!/bin/bash
systemctl reload nginx haproxy
EOF
chmod +x /etc/letsencrypt/renewal-hooks/post/reload.sh
```

16.2 Cron Alternative

```
0 */12 * * * root certbot renew --quiet \
  --post-hook "systemctl reload nginx haproxy"
```

16.3 Testing Renewal

```
certbot renew --dry-run
```

Check `/var/log/letsencrypt/letsencrypt.log` for errors and configure email alerts on failure.

17 Licensing Requirements

Ensure compliance for all software components:

- **Hypervisor:** Valid support contracts for VMware ESXi, Hyper-V, etc.
- **Windows VMs:** Appropriate RDS CALs or equivalent licensing per concurrent user.
- **Certificates:** Trusted CA-signed TLS certificates (Let's Encrypt or commercial).
- **HAProxy Enterprise:** Optional subscription for advanced modules; community edition is free.

18 Routine Maintenance

18.1 Quarterly Tasks

- Reboot gateway and hosts every 3-4 months to apply kernel and firmware updates.
- Review and apply OS and application patches.

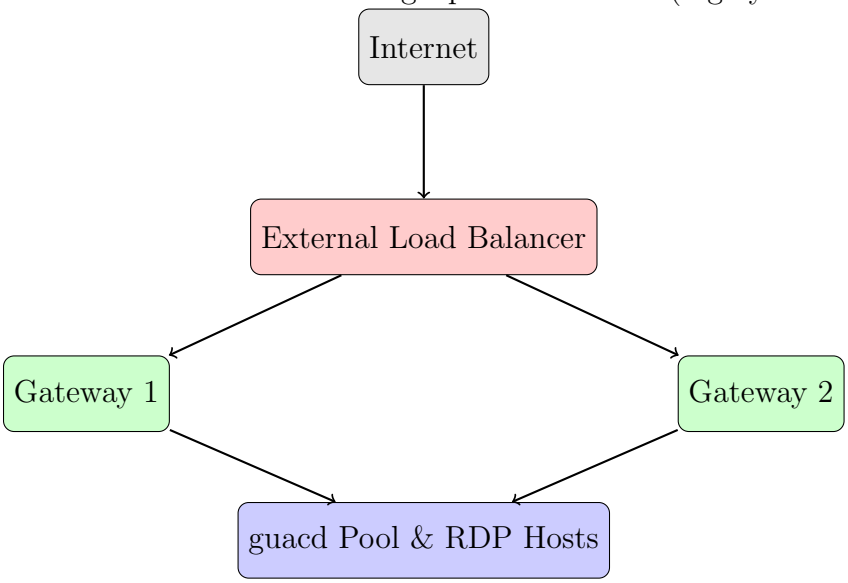
18.2 Service Recovery

```
sudo systemctl start guacd guacamole nginx haproxy
```

19 Security and Compliance

19.1 High Availability & DR (Section 19.1)

For deployments requiring >200 concurrent sessions, deploy multiple gateways behind a load balancer to eliminate single points of failure (highly recommended). Example topology:



19.2 Monitoring & Alerting (Section 19.2)

Detailed recommendations for proactive monitoring and alerting (highly recommended):

- **Metrics to collect:** CPU usage, memory
- **Exporters:** Prometheus Node Exporter, HAProxy Exporter (port 8405), Guacamole JMX exporter.
- **Dashboards:** Grafana panels for real-time session trends, resource utilization, backend health.
- **Alert rules:**
  - CPU >80% for 5 minutes.
  - Memory >75% for 10 minutes.
  - Session failures >5 in 1 minute.
  - HAProxy backend down events.
- **Notifications:** Email, Slack, PagerDuty for critical alerts.
- **Retention:** Store metrics for at least 90 days for capacity planning.

19.3 Security Hardening (Section 19.3)

Highly recommended: Install and configure Fail2Ban for SSH, HTTPS, and RDP; enable AppArmor profiles for `nginx`, `guacd`, and `haproxy`. Regularly review logs for intrusion attempts.

19.4 Compliance & Auditing (Section 19.4)

Highly recommended: Enable the session recording extension in Guacamole to archive logs/recordings for FERPA compliance. Store audit logs centrally and enforce retention policies.

20 Customizing Theme and Branding

The most effective way to customize Guacamole's appearance is through a proper extension JAR file:

1. Install Java JDK for JAR creation:

   ```
   sudo apt update && sudo apt -y install default-jdk
   ```

2. Create a theme project directory:

   ```
   mkdir -p ~/guac-theme-builder/{css,images,translations,META-INF}
   cd ~/guac-theme-builder
   ```

3. Create required files:

   a. `META-INF/MANIFEST.MF`:

   ```
   Manifest-Version: 1.0
   Guacamole-Extension-Name: School District Branding
   Guacamole-Extension-Namespace: district-branding
   ```

   b. `guac-manifest.json`:

   ```
   {
     "name" : "School District Branding",
     "namespace" : "district-branding",
     "cssResources" : [
       "css/custom-theme.css"
     ],
     "resources" : {
       "images/logo.png" : "image/png",
       "images/favicon.png" : "image/png"
     },
     "smallIcon" : "images/favicon.png"
   }
   ```

   c. `css/custom-theme.css`:

   ```
   .login-ui .login-dialog .logo {
       background-image: url('app/ext/district-branding/images/logo.png');
       width: 7em;
   ```

```
    height: 7em;
    -webkit-background-size: 7em auto;
}

#login-header {
    background: #00457c;
}
```

4. Add your district logo:

```
cp /path/to/your/logo.png images/logo.png
cp /path/to/your/favicon.png images/favicon.png
```

5. For users preferring a GUI approach, 7-zip is the easiest way to handle JAR file creation and updates. Simply:
   - Create a ZIP file with all your theme files maintaining directory structure
   - Ensure the MANIFEST.MF file is in the META-INF directory
   - Rename the .zip file to .jar
6. For command-line users, build and install the extension:

```
jar cfmv branding.jar META-INF/MANIFEST.MF guac-manifest.json \
    css images translations META-INF
sudo mv branding.jar /etc/guacamole/extensions
sudo chmod 664 /etc/guacamole/extensions/branding.jar
```

7. Restart Guacamole services:

```
TOMCAT=$(ls /etc/ | grep tomcat)
sudo systemctl restart guacd && sudo systemctl restart ${TOMCAT}
```

8. Clear your browser cache and refresh the page to see your changes.

Theme Customization Tips:

- Maintain the directory structure shown above.
- The `namespace` value in guac-manifest.json must match the namespace used in CSS URLs.
- For logos, provide multiple sizes for different displays.
- Use browser developer tools to preview and debug style changes.
- If changes don't appear, clear browser cache before troubleshooting further.

21 Conclusion

You now have a production-ready, school-branded remote desktop solution:

- **Secure Access:** AD-integrated SSO, TLS encryption, VLAN isolation, and brute-force protection.
- **Scalable Architecture:** Properly sized gateway VMs, HAProxy load balancing, and optional GPU passthrough.
- **Operational Simplicity:** Automated certificate renewals, quarterly maintenance checklist, and clear recovery steps.
- **Visibility and Compliance:** Real-time monitoring, alerting, session recording, and audit trails.

Next steps:

- Integrate additional protocols (SSH, VNC) for broader use cases.
- Explore HAProxy Enterprise modules for advanced traffic management.
- Train staff on usage and maintenance procedures.