

Proxy Server Security Comparison: Current vs New Implementation

Quick Comparison Table

Security Aspect	Current Server	New Plan
Password Storage	Plain text (exposed)	Hashed (nonce)
Authentication Method	Basic (cleartext)	Digest + IP-based
User Management	Shared credentials	Individual accounts
Site Blocking	None	Enabled
Office Access	Username/Password	IP-based (automatic)
Remote Access	Username/Password	Digest authentication
User Tracking	No trackability	Full traceability

Current System Critical Issues

Security Vulnerabilities

- Exposed Credentials: Username and password visible on internet
- Cleartext Transmission: Basic authentication sends credentials unencrypted
- Shared Accounts: Multiple users using same login credentials
- No Access Control: Unrestricted internet access without site blocking
- Zero Accountability: Cannot track individual user activities

New Plan Security Enhancements

Authentication Improvements

- Digest Authentication: Encrypted credential transmission for remote users
- IP-Based Office Access: Seamless authentication for office users
- Individual User Accounts: Unique credentials for each user

Access Control Features

- **Site Blocking:** Content filtering to block malicious and inappropriate websites
- **Comprehensive Logging:** Full audit trail of all user activities
- **User Accountability:** Complete traceability of actions to individuals
- **TLS/SSL Encryption:** - Full Encryption: TLS ensures that both user traffic, TLS adds confidentiality, integrity,

DNS domain created in AWS route 53:

The screenshot shows the AWS Route 53 console for a hosted zone named **d3nniplayz.click**. The zone is public and has three records:

Record name	Type	Routing policy	Alias	Value/Route traffic to	TTL (seconds)	Health check
d3nniplayz.click	NS	Simple	No	ns-1845.awsdns-38.co.uk. ns-464.awsdns-58.com. ns-567.awsdns-06.net. ns-1367.awsdns-42.org.	172800	-
d3nniplayz.click	SOA	Simple	No	ns-1845.awsdns-38.co.uk. a...	900	-
proxy.d3nniplayz.click	A	Simple	No	50.18.91.153	300	-

Digest Auth:

The screenshot shows a Wireshark network capture of a Digest Authentication request. The selected packet is a **HTTP 407 Proxy Authentication Required** message. The **Details** pane shows the **Proxy-Authenticate** header with the following values:

```
Proxy-Authenticate: Digest username="denni",  
realm="Squid Proxy",  
nonce="b42af6b0c8de123a389ff11477da711",  
uri="token.rubiconproject.com:443",  
response="b2bacf6a90bc8a8657b7a1eb12567f7",  
qopauth  
nc=00000022
```

The **Packet Bytes** pane shows the raw data of the packet, which is a **Text item (text), 2 bytes**.

Traffic Encrypted using TLS/SSL certificate:

The image shows a Wireshark packet capture of an HTTP connection. The top pane displays a list of packets, with packet 35350 selected. The middle pane shows the details of the selected packet, including the Hypertext Transfer Protocol, Transport Layer Security (TLSv1.3), and the Encrypted Application Data. The bottom pane shows the packet bytes. The right pane displays a packet diagram showing the structure of the TLSv1.3 record, including the Hypertext Transfer Protocol, Transport Layer Security, and the Encrypted Application Data.

No.	Time	Source	Destination	Protocol	Length	Info
35119	1706.045126	192.168.0.227	50.18.91.153	TLSv1.3	263	Application Data
35124	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1514	Application Data
35125	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1514	Application Data
35126	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1514	Application Data
35127	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1514	Application Data
35128	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1514	Application Data
35129	1706.288827	50.18.91.153	192.168.0.227	TLSv1.3	1418	Application Data, Application Data, Application Data
35131	1706.289278	192.168.0.227	50.18.91.153	TLSv1.3	93	Application Data
35342	1714.479942	192.168.0.227	50.18.91.153	HTTP	521	CONNECT kyrhcaapp.ecwcloud.com:443 HTTP/1.1
35348	1714.773990	50.18.91.153	192.168.0.227	HTTP	96	HTTP/1.1 200 Connection established [Malformed Packet]
35349	1714.774514	192.168.0.227	50.18.91.153	TCP	1514	64078 → 6969 [ACK] Seq=468 Ack=40 Win=65280 Len=1460 [TCP PDU reassembled in 35350]
35350	1714.774514	192.168.0.227	50.18.91.153	TLSv1.3	501	Client Hello (SN=kyrhcaapp.ecwcloud.com)
35352	1715.068542	50.18.91.153	192.168.0.227	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
35354	1715.068542	50.18.91.153	192.168.0.227	TLSv1.3	1164	Application Data, Application Data, Application Data
35356	1715.072947	192.168.0.227	50.18.91.153	TLSv1.3	134	Change Cipher Spec, Application Data
35357	1715.073773	192.168.0.227	50.18.91.153	TLSv1.3	571	Application Data
35360	1715.350379	50.18.91.153	192.168.0.227	TLSv1.3	660	Application Data, Application Data
35362	1715.582016	50.18.91.153	192.168.0.227	TCP	1514	6969 → 64078 [ACK] Seq=4696 Ack=2972 Win=77440 Len=1460 [TCP PDU reassembled in 35368]

Connect using the dns

The image shows the Squid proxy configuration window. The "Configure Proxy Access to the Internet" section is active, and the "Manual proxy configuration" option is selected. The HTTP Proxy is set to "proxy.d3nniplayz.click" and the Port is 6969. The checkbox "Also use this proxy for HTTPS" is checked. The HTTPS Proxy is also set to "proxy.d3nniplayz.click" and the Port is 6969. The SOCKS Host is empty and the Port is 0. The "Automatic proxy configuration URL" is set to "http://proxy.d3nniplayz.click:6969/". The "No proxy for" section is empty. The "Example: .mozilla.org, .net.nz, 192.168.1.0/24" is shown. The "Connections to localhost, 127.0.0.1/8, and ::1 are never proxied." is noted. The "Do not prompt for authentication if password is saved" checkbox is unchecked. The "Proxy DNS when using SOCKS v4" checkbox is unchecked. The "Proxy DNS when using SOCKS v5" checkbox is checked. The "OK" and "Cancel" buttons are at the bottom.

Add the squid config file and other dependent file in github.