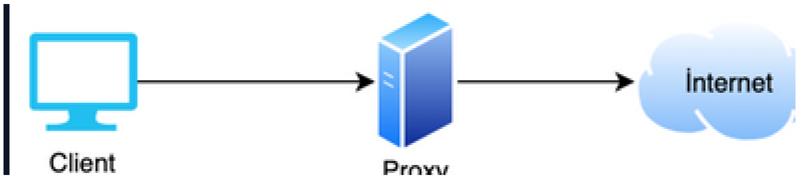
VPN Log Analysis Questions

By: Ryan Stewart



VPN Log Details

- **date**: Date
- **time**: Time
- **devname**: Hostname
- **devid**: Device ID
- **eventtime**: Event timestamp
- **tz**: Time zone
- **logid**: Log ID
- **type**: Log Type (traffic, utm, event, etc.)
- **subtype**: Sub Log Type (Forward, vpn, webfilter, virus, ips, system, etc.)
- **level**: Log level
- **logdesc**: Log description
- **action**: Action taken
- **tunneltype**: VPN tunnel type
- **remip**: IP address establishing the VPN connection
- **user**: User information
- **reason**: VPN Connection Request Result
- **msg**: Detailed message after the access

Analyzing VPN Logs

The critical information to examine in VPN logs includes the connecting IP address, associated user, and the result of the access request. After a successful VPN connection, an IP is assigned for access. This IP information may be included in the same log or in a separate log.

Use Case: Phishing Attack Response

In scenarios like a phishing attack targeting an organization, analysts may need to scrutinize VPN logs for users who may have inadvertently disclosed credentials. Suspicious activities detected through VPN logs include:

- Successful/Unsuccessful VPN accesses
- Brute-force attacks against VPN accounts
- VPN accesses outside specified countries
- VPN accesses outside specified time periods

Traffic Log Integration

Firewall traffic logs are crucial for VPN analysis. The `srcip` in the traffic log matches the `remip` values in the VPN log. For instance, the application (service) information in the traffic log may indicate HTTPS for an SSL-VPN type.

Understanding the correlation between VPN and firewall logs enhances the ability to investigate and respond to potential security incidents effectively.

VPN Quiz

Question 1: VPN only works on firewall devices. False

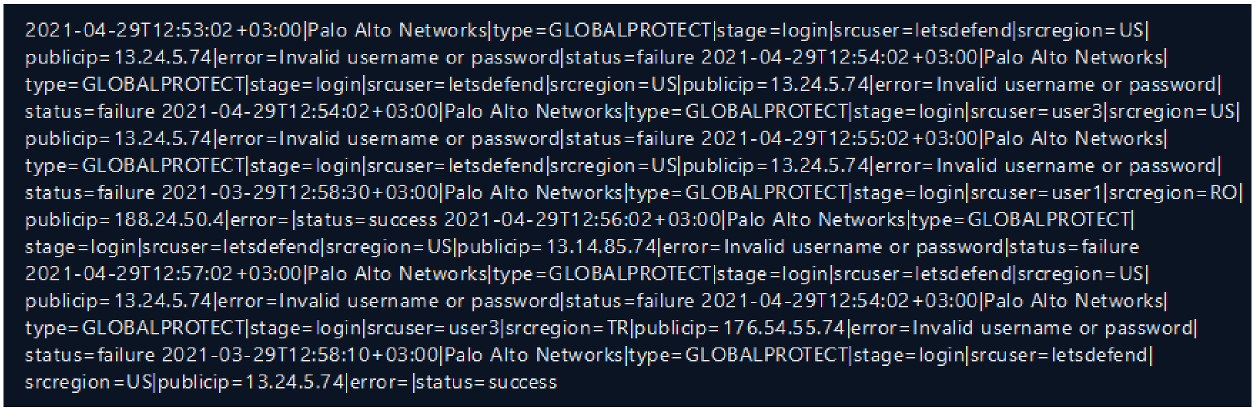
Question 2: Which of the following is not a type of VPN?

A) SSL-VPN
B) Site-to-Site VPN
C) IPSec VPN
D) DNS over VPN

Question 3: Which one is true for the "letsdefend" user logs?

A) Brute-Force Attack
B) 4 Successful VPN connections were established with Letsdefend user

C) Letsdefend user has successfully logged in from DE location



```
2021-04-29T12:53:02 +03:00|Palo Alto Networks|type=GLOBALPROTECT|stage=login|srcuser=letsdefend|srcregion=US|
publicip=13.24.5.74|error=Invalid username or password|status=failure 2021-04-29T12:54:02+03:00|Palo Alto Networks|
type=GLOBALPROTECT|stage=login|srcuser=letsdefend|srcregion=US|publicip=13.24.5.74|error=Invalid username or password|
status=failure 2021-04-29T12:54:02+03:00|Palo Alto Networks|type=GLOBALPROTECT|stage=login|srcuser=user3|srcregion=US|
publicip=13.24.5.74|error=Invalid username or password|status=failure 2021-04-29T12:55:02+03:00|Palo Alto Networks|
type=GLOBALPROTECT|stage=login|srcuser=letsdefend|srcregion=US|publicip=13.24.5.74|error=Invalid username or password|
status=failure 2021-03-29T12:58:30+03:00|Palo Alto Networks|type=GLOBALPROTECT|stage=login|srcuser=user1|srcregion=RO|
publicip=188.24.50.4|error=|status=success 2021-04-29T12:56:02+03:00|Palo Alto Networks|type=GLOBALPROTECT|
stage=login|srcuser=letsdefend|srcregion=US|publicip=13.14.85.74|error=Invalid username or password|status=failure
2021-04-29T12:57:02 +03:00|Palo Alto Networks|type=GLOBALPROTECT|stage=login|srcuser=letsdefend|srcregion=US|
publicip=13.24.5.74|error=Invalid username or password|status=failure 2021-04-29T12:54:02+03:00|Palo Alto Networks|
type=GLOBALPROTECT|stage=login|srcuser=user3|srcregion=TR|publicip=176.54.55.74|error=Invalid username or password|
status=failure 2021-03-29T12:58:10+03:00|Palo Alto Networks|type=GLOBALPROTECT|stage=login|srcuser=letsdefend|
srcregion=US|publicip=13.24.5.74|error=|status=success
```

Question 4: Which of the following is true for the “user3” VPN User?

A) Brute-Force Attack
B) user3 made a successful VPN connection
C) There were failed login attempts from different locations within a short period of time
D) user3 made a successful VPN connection from the US location