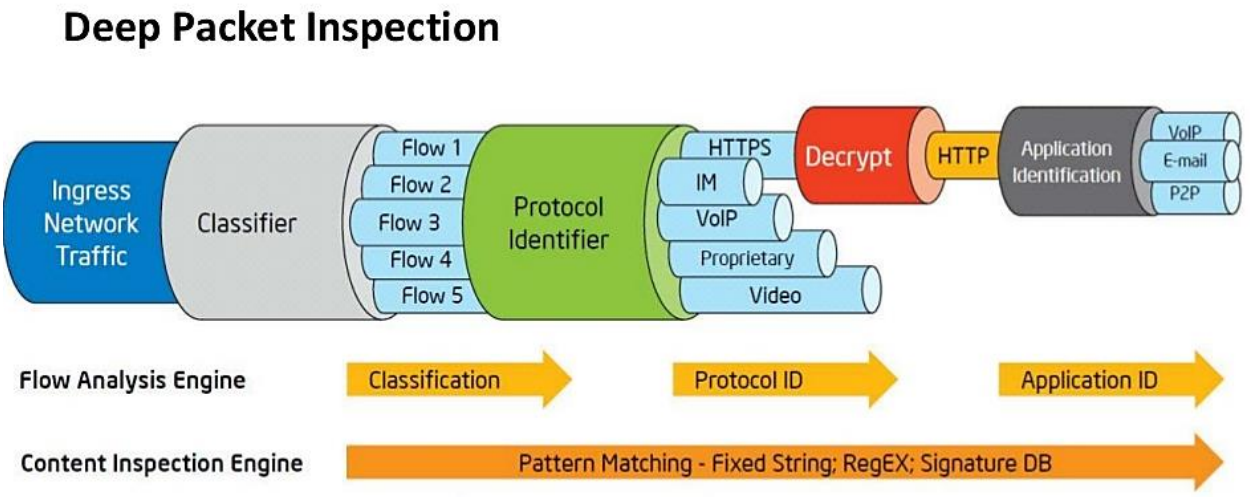
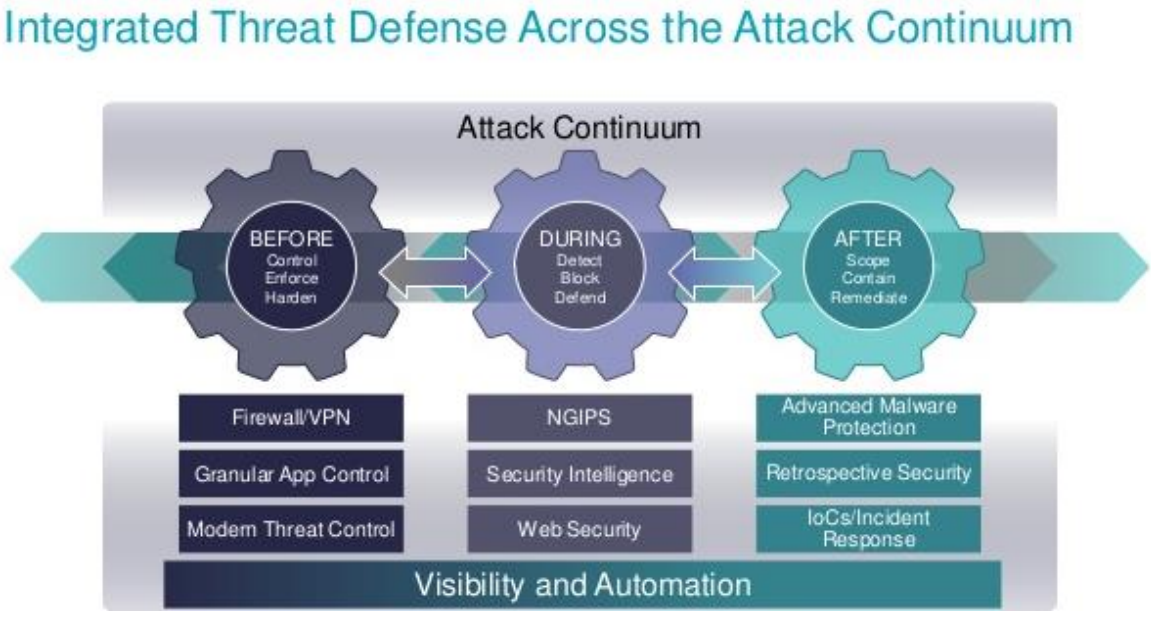
## Next-Generation Firewall (NGFW):

- NGFW performs the role of a traditional firewall and adds the NGIPS features.
- Next-Generation Firewall is part of the third generation of Firewall technology.
- All NGFWs offer two key features App Awareness and Control & ID Awareness.
- Next-Generation Firewall (NGFW) provide deep-packet inspection of the traffic.
- Next-Generation Firewall add application-level inspection & Intrusion Prevention.
- Next-Generation Firewall provides all traditional IPS features with high performance.
- Next-Generation Firewall allow, and block traffic based on specific application as well.
- Next-Generation Firewall allow, and block traffic based on user information as well.
- Next-Generation Firewall (NGFW) provide both IPS and application control functions.
- There is no big difference between the UTM and Next-Generation Firewall (NGFW).
- Next-Generation Firewall provide high performance and Processing using to protect.






https://t.me/learningnets

## App-ID (Application Identification):

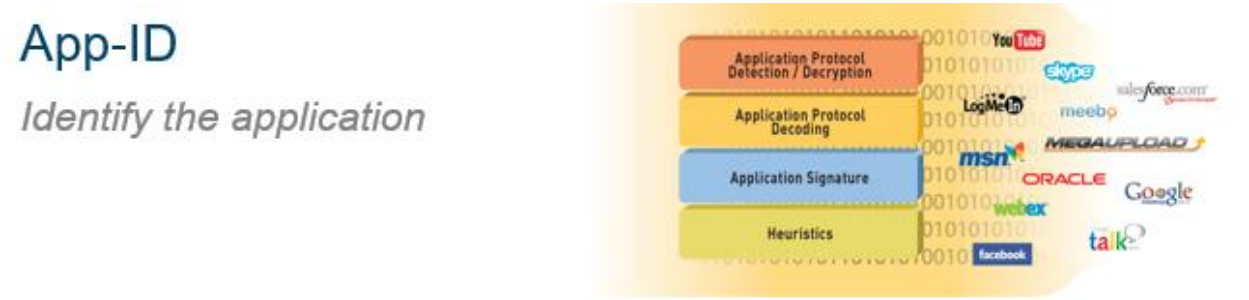
Is a combination of application signatures, protocol detection and decryption, protocol encoding, and heuristics to identify Applications. This application identification is carried through to the Content-ID functionality to scan and inspect applications appropriate to their use as well as to the policy engine.

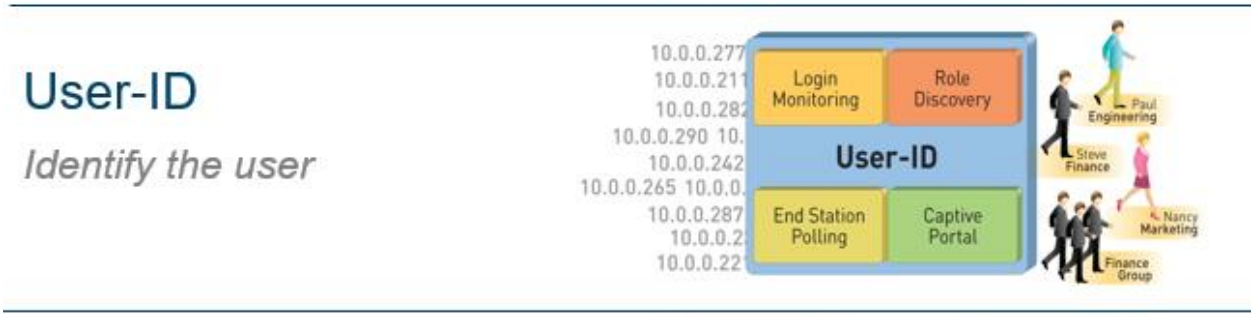
## Content-ID (Scan Content):

Single hardware accelerated signature format to scan traffic for data credit card numbers, social security numbers, and custom patterns and Threats vulnerability exploits -IPS, viruses and spyware plus a URL categorization engine to perform URL Filtering.

## User-ID (Identify User):

Maps IP Address to Active Directory users and users to groups (roles) to enable visibility and policy enforcement by user and group.



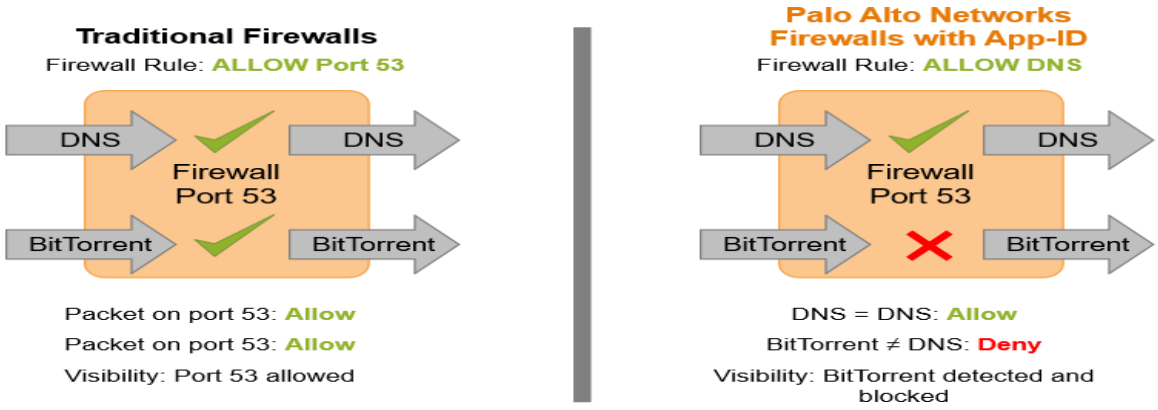




**https://t.me/learningnets**

## APP-ID:

- Application Identification or App-ID is a main component of Palo Alto devices.
- Traditional Firewalls classify traffic by port and protocol, PA Firewall Use App-ID.
- Application is specific program whose communication can be labeled & monitored.
- Application is specific feature whose communication can be labeled and controlled.
- Port-based rules use Service; App-ID or Application-based rules use the application.
- Application rules allow only the application traffic that is allowed & no other traffic.
- Unknown traffic trying to pass application policy is blocked, because it doesn't match.
- Application Identity for UDP can generally identify the application on the first packet.
- App-ID for TCP take several packets to identify, as 3-way handshake needs to be done.
- Then the application data will need to be examined, depending on the application data.
- Application Database is updated weekly with new and updated application identifiers.
- App-ID identification of applications ensures the success of proper Layer 7 inspections.
- Application Signatures today over 3,000, Application Protocol Decoders, and heuristics.
- These elements are responsible for visibility of L7 traffic traversing P Networks firewalls.
- Apps are categorized and classified by App-ID engine, allowing proper identification.
- During classification process, Palo Alto Networks defines main applications (Parent App).
- Some directly dependent (or Child App), which are part of these main applications.
- Link to verify Application Identity or inside firewall applipedia.paloaltonetworks.com.

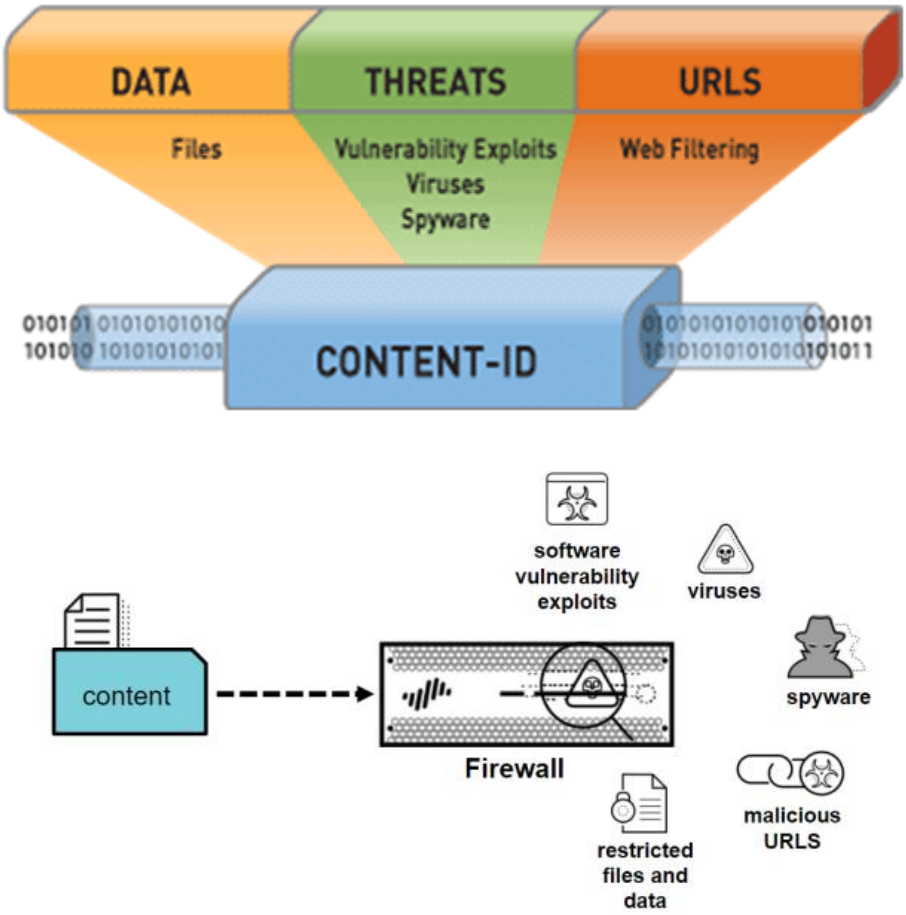






https://t.me/learningnets

## Content-ID:

- Content-ID is a content inspection appliance that prevents a wide range of threats.
- Content-ID blocks unauthorized file and data transfers, and controls web surfing.
- Provides a real-time threat prevention engine, combined with full URL database.
- Threat prevention engine & policies inspect and control content traversing Firewall.
- PA Firewall in content filtering first priority is given to URL filtering in security group.
- Action on the rule needs to be allowed before it can process the Antivirus check.

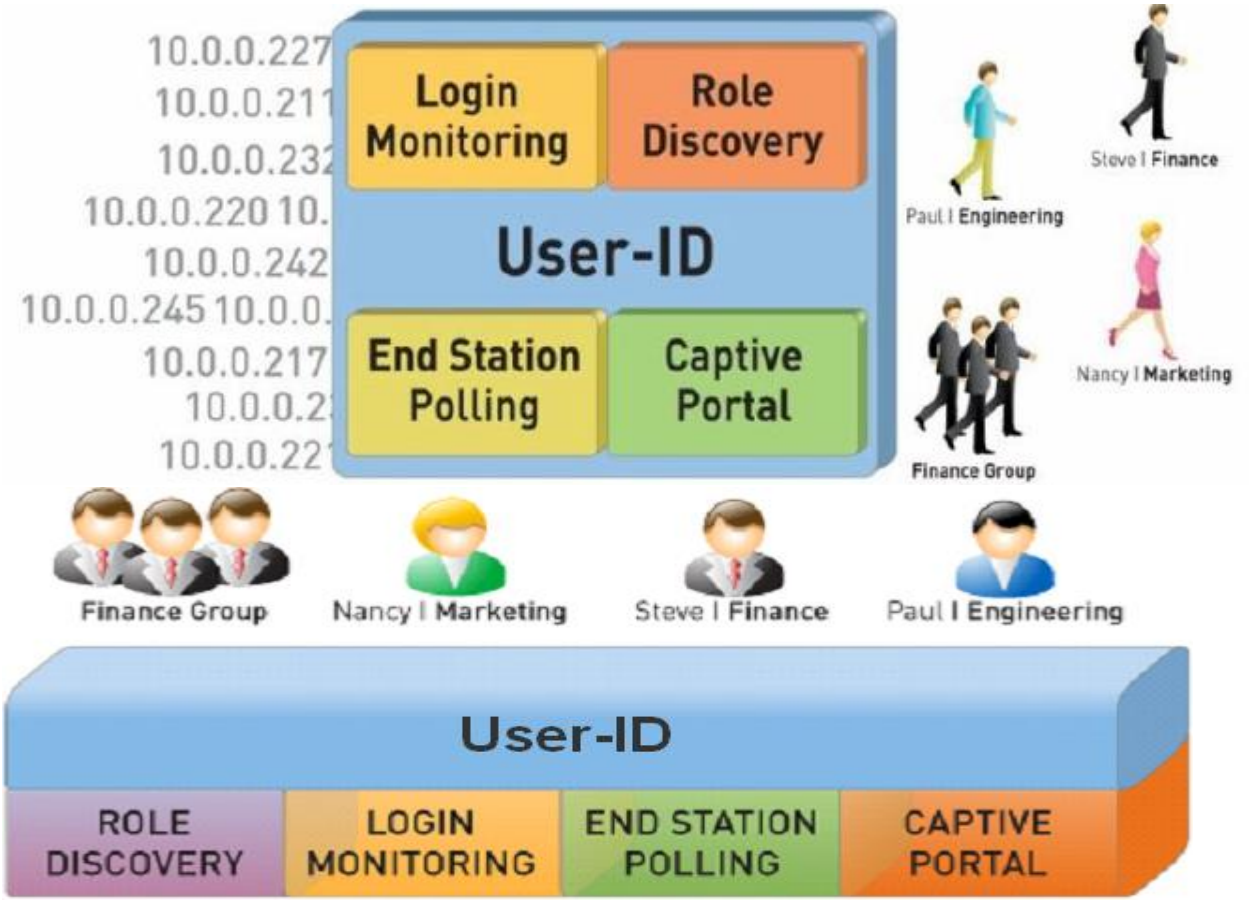





https://t.me/learningnets

## User-ID (User Identification):

- Security infrastructure is based on three pillars application, user and content.
- The User Identification is a Palo Alto Networks next-generation firewall feature.
- User-ID, as opposed to IP address, is integral component of security infrastructure.
- User-ID, knowing which who is using each of the applications on your network.
- Who have transmitted threat or transferring files can strengthen security policies.
- User-Id technology not only identifies users with usernames but also IP Address.
- Create policies & display logs and reports based on usernames and group names.
- User-ID technology provide Visibility, Policy control, & Logging, reporting, forensics.
- Firewall collects Group Mapping info by connecting directly to LDAP directory server.
- Visibility into what users are doing on the network becomes increasingly important.
- Full visibility into user activity on the network & user-based policy control & reporting.
- Improved visibility into application usage and more relevant picture of network activity.
- Configuring User-ID enables ACC, App Scope, reports, and logs to include usernames.
- User-ID enables you to identify all users on your network using a variety of techniques.
- User-ID, when tied to the application activity, provides you with more complete visibility.
- Greater policy control, and more granular logging, reporting and forensics capabilities.
- Main things provide by User-ID is Visibility, Policy control & Logging, reporting, forensics.
- User-ID integrates Palo Alto firewall functionality with wide range of user repositories.






https://t.me/learningnets