OMEGA TELESERVE, LLC

Next-Gen Firewall Feature Descriptions

Application Control

- Ability to recognize and control traffic for over 2,600 applications
- Policy triggers for applications, application groups or application filters
- Ability to combine policy triggers with each other using and/or logic
- Ability to apply actions (allow, deny, reject) or profiles (IP filtering, file filtering, DNS filtering, URL filtering, etc.) to specific criteria
- Application control features are available for all policy types

User and Group Definition and Control

- Active Directory and LDAP support
- Authentication support for Kerberos or based on forms via captive portal using LDAP
- User, group or attribute policy triggers
- Ability to combine policy triggers with each other using and/or logic
- Ability to apply actions or profiles to specific criteria
- Application control features are available for all policy types: Access, QoS, PBF, traffic monitoring, SD-WAN

SSL Inspection

- Security checks for expired certificates; untrusted issuers; unsupported ciphers, key lengths or versions; restrict certificate extensions
- Allow, deny, reject, alert (allow & log) actions

IP Reputation & Filtering

- Geo-location
    - Enforce actions based on source IP, destination IP or both, based on global IP address database

- IP Reputation
    - Protection against over 12 million malicious IPv4 and IPv6 IP addresses
    - Supports user-defined black & white lists
    - Updates in near real time
    - Match based on source IP, destination IP or both

URL Reputation and Filtering

- Classification of over 460 million domains and 13 billion URLs
- 83 predefined categories with custom & cloud app category support
- Supports user-defined black & white lists
- Real-time lookups of URL categories & reputation
- URL and URL category policy triggers
- Triggers can be combined with other match conditions (and, or)
- Apply actions to allow, deny, reject, log, QoS, inform, ask, notify, override, block or apply profile
- Available for all policy types: access, QoS, PBF, monitoring, authentication, decryption, SD-WAN

DNS Reputation & Filtering

- DNS-based protection & access control
  - Policy triggers from DNS query data
  - Combined with Zones, IP Addresses, Geo-Location, User/Group, Category, Reputation
  - Supports user-defined black & white lists
  - Actions include Allow, Deny, Reject, Log, QoS
- Global DNS Intelligence for zero-day threats
- Passive DNS database
- Block resolution of new domains until reputation is updated
- Internal names, brand spoofing: provides enhanced phishing protection through potentially suspect sites or DNS configuration errors
- Integration with URL Category and IP Reputation Feeds