NET3900: Assignment 5

These questions are based on Module 5. Submit your answers via Bb by end-of-day Thursday October 13, 2016. Always show your calculations or provide explanation for your answers. The marks value for each question follows the question number.

1/3. Consider the following session policy:

```
1 netdestination dns-srv
2 host 10.252.1.20

3 ip access-list session NewPolicy
4    user network 10.254.0.0 255.255.0.0 any permit
5    user host 10.254.1.20 any deny
6    user alias dns-srv any permit
```

Will the policy permit or deny the following packets and which statement will perform the action?

```
a) Source IP = user; Dest IP = 10.254.1.20
b) Source IP = user; Dest IP = 10.253.1.20
c) Source IP = user; Dest IP = 10.252.1.20
```

a) permit, statement 4
b) deny, implicit deny at end
c) permit, statement 6

2/3. User Roles are defined using Firewall Session Policies. Briefly describe (in your own words) the three advantages of Firewall Session Policies over regular ACLs.

a) Stateful: recognize flows and track session states (ie. TCP session)
b) Bi-directional: tracks traffic direction. If packet goes out, then policy knows to permit the response. (ie if you permit "user host echo", then the echo reply will be permitted)
c) Dynamic: Key words are parameters which change value depending on the user. (ie. "user" changes value depending on IP address of connected user).

3/3. Briefly describe the steps in the 802.1X/PEAP negotiation. This is shown as Part B on slide 36.

1. Client request and gets server certificate. Certificate is validated.
2. Client and RADIUS server user public/private keys to set up encrypted TLS tunnel
3. Client sends username and password in encrypted tunnel. RADIUS validates
4. Client and RADIUS creaste PMK (pairwise master key) for encryption.
5. Tunnel Teardown

4/3. Describe the three steps to validate a certificate.
1. Decript the Cert using the Cert Authority Public Key. This results in a HASH
2 Create a new HASH of the Certificate.
3. If the two HASH values match then validated

5/4. Describe the role of the public and private keys of the Certificate Authority and the public and private keys of the Enterprise server certificate. One or two sentences description for each should be sufficient.
1. CA Private Key: Used to Encrypt (ie Sign) the Enterprise Certificate
2. CA Public Key: Used by user devices to decrypt the Digital Signature
3. Enterprise Public Key: Sent in Certificate with Digital Signature to validate the server.
4. Enterprise Public Key: Used in conjunction with Enterprise Key to securely create encryption key.

6/3. A malicious person uses the following method to forge credentials for a rogue server. They connect to a valid server and authenticate (using 802.1X/PEAP) to get the valid server's public key certificate already signed by the Certificate Authority (CA). This stolen certificate is now loaded onto the rogue server. The public key certificate from the CA is already loaded on user computing devices. Will this work? Why or Why not?
It will not work for the following reason. The certificate will authenticate. But the correct Enterprise Private key is not loaded on the server so the data encryption will fail.