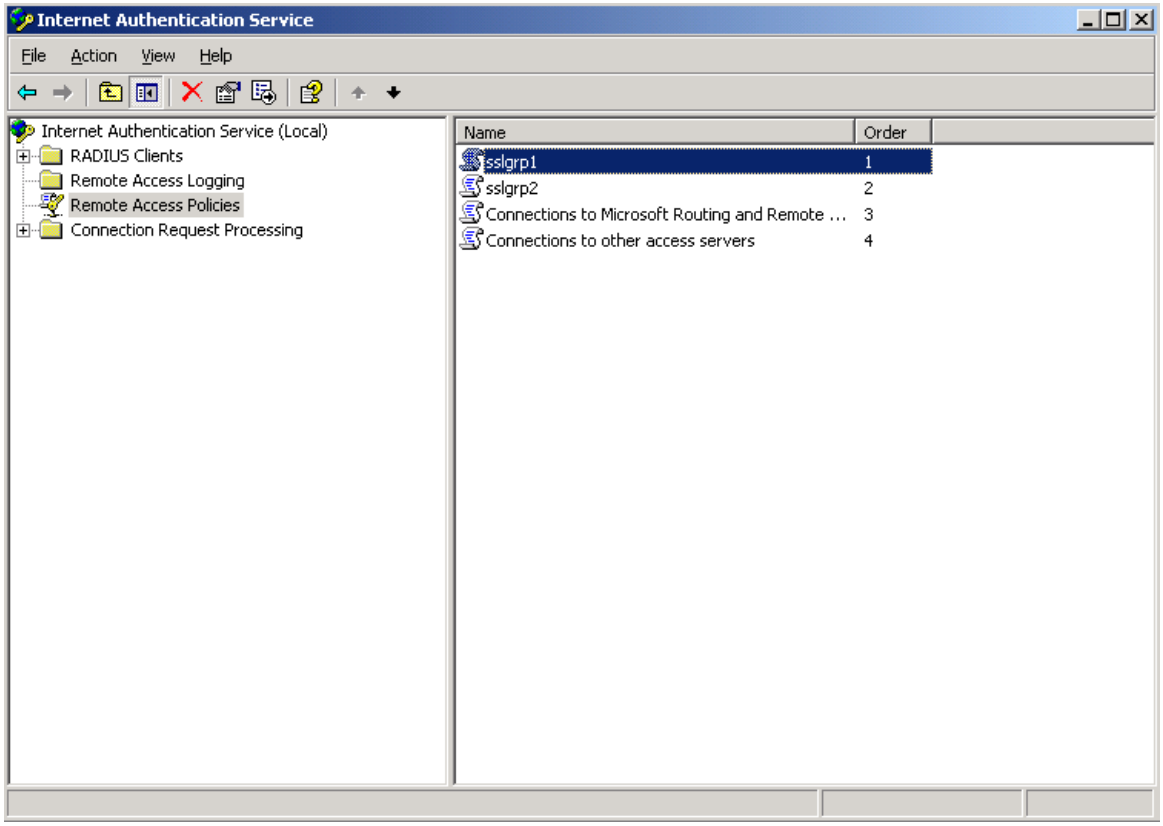
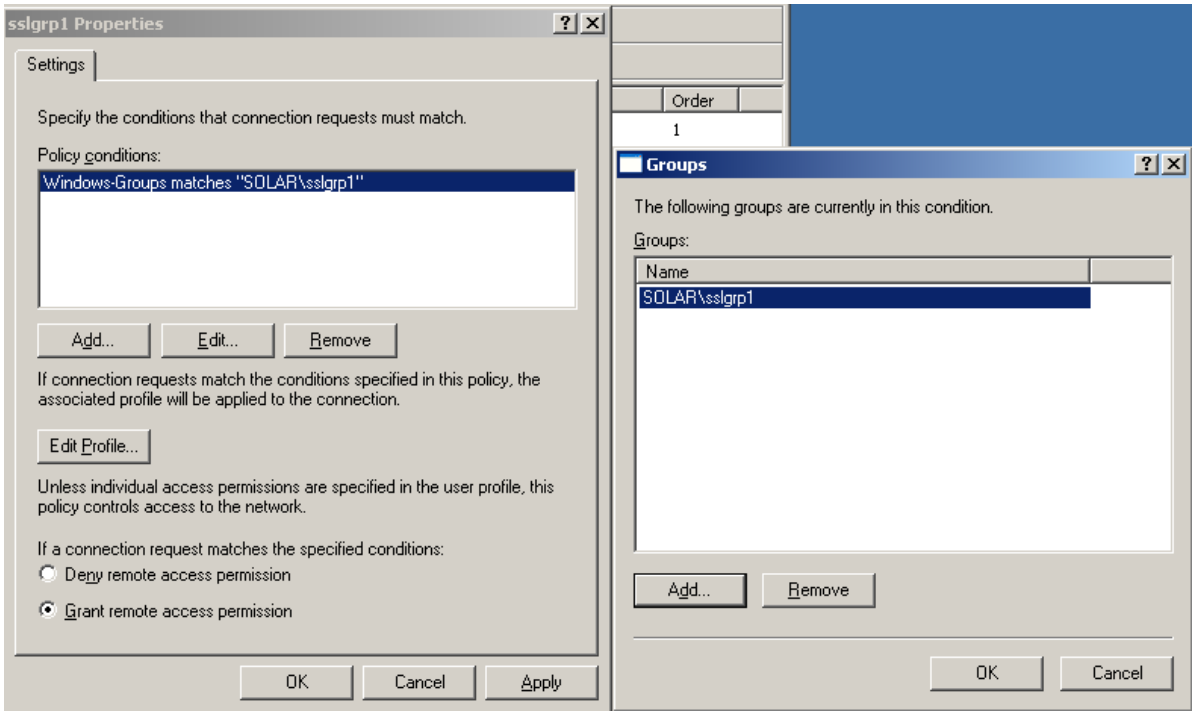
This document consists of a series of screen shots that show how to import Fortinet RADIUS Vendor-Specific Attributes (VSAs) into Windows 2003 server. This document also shows the FortiGate configuration and shows the content of some example RADIUS packets.

1. Importing FortiGate VSAs into Windows 2003 Server

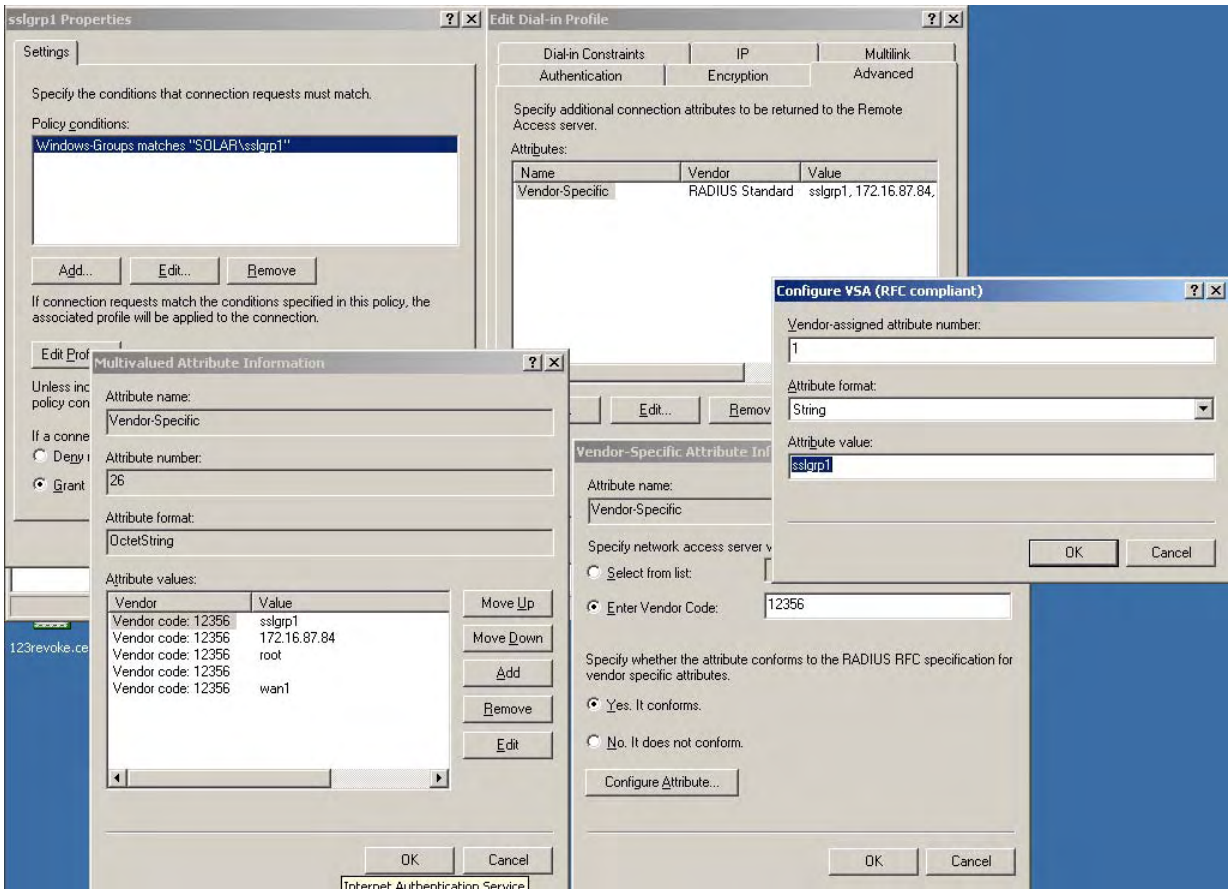
Step 1



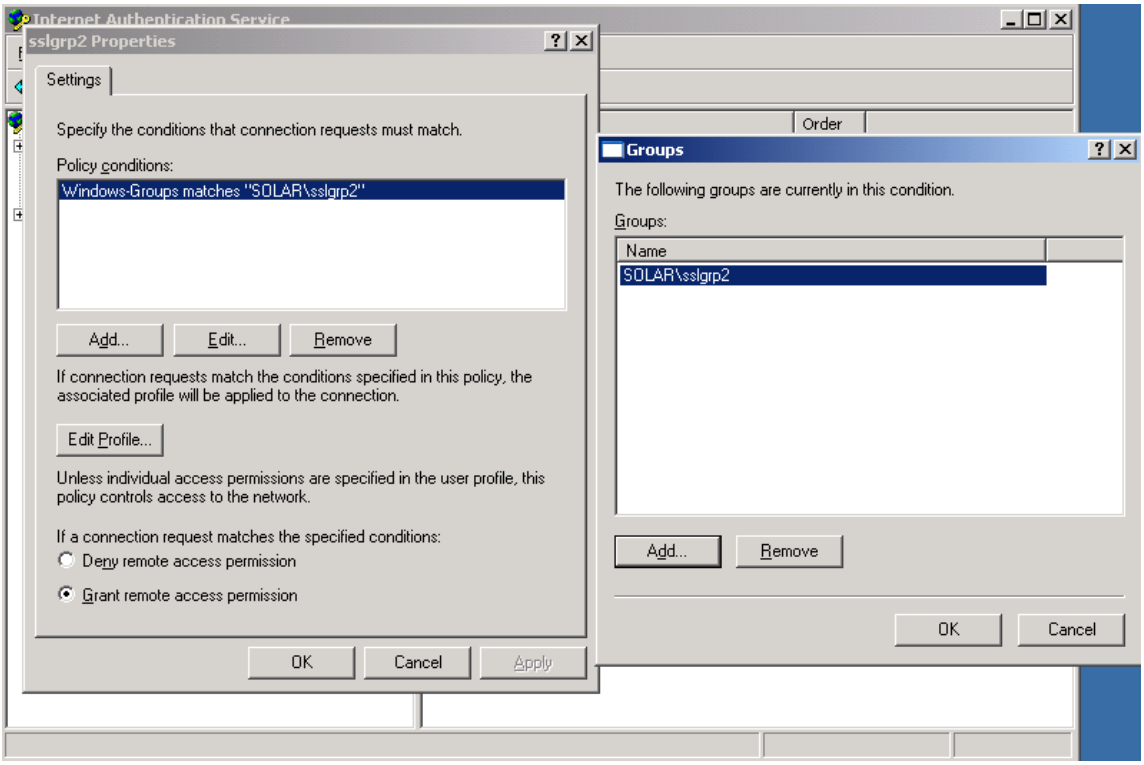
Step 2


sslgrp1 Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Windows-Groups matches "SOLAR\sslgrp1"
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Profile...
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission
OK
Cancel
Apply
Order
1
Groups
The following groups are currently in this condition.
Groups:
Name
SOLAR\sslgrp1
Add...
Remove
OK
Cancel

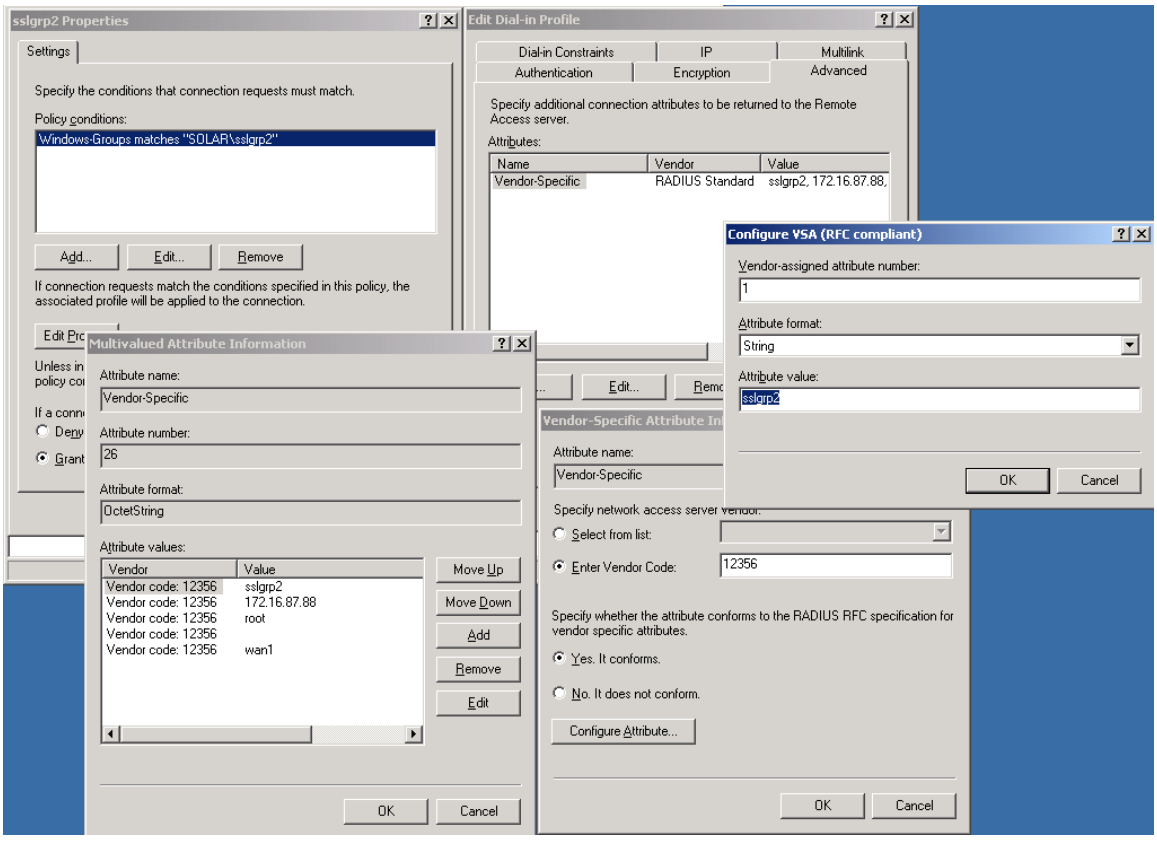
Step 3


sslgrp1 Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Windows-Groups matches "SOLAR\sslgrp1"
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Specify additional connection attributes to be returned to the Remote Access server.
Attributes:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
sslgrp1, 172.16.87.84,
Multivalued Attribute Information
Attribute name:
Vendor-Specific
Attribute number:
26
Attribute format:
OctetString
Attribute values:
Vendor
Value
Vendor code: 12356
sslgrp1
Vendor code: 12356
172.16.87.84
Vendor code: 12356
root
Vendor code: 12356
Vendor code: 12356
wan1
Move Up
Move Down
Add
Remove
Edit
OK
Cancel
Configure VSA (RFC compliant)
Vendor-assigned attribute number:
1
Attribute format:
String
Attribute value:
sslgrp1
OK
Cancel
Vendor-Specific Attribute Inf
Attribute name:
Vendor-Specific
Specify network access server
Select from list:
Enter Vendor Code:
12356
Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.
Yes. It conforms.
No. It does not conform.
Configure Attribute...
OK
Cancel

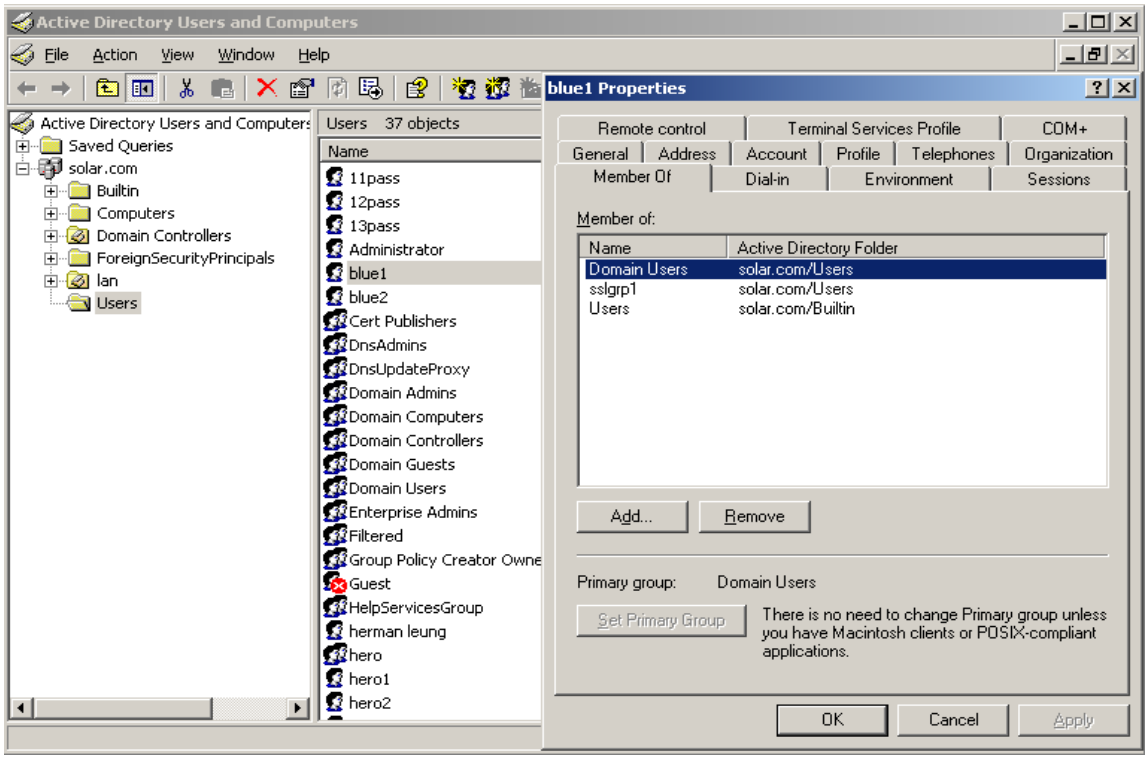
Step 4


Internet Authentication Service
sslgrp2 Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Windows-Groups matches "SOLAR\sslgrp2"
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Profile...
Unless individual access permissions are specified in the user profile, this policy controls access to the network.
If a connection request matches the specified conditions:
Deny remote access permission
Grant remote access permission
OK
Cancel
Apply
Order
Groups
The following groups are currently in this condition.
Groups:
Name
SOLAR\sslgrp2
Add...
Remove
OK
Cancel

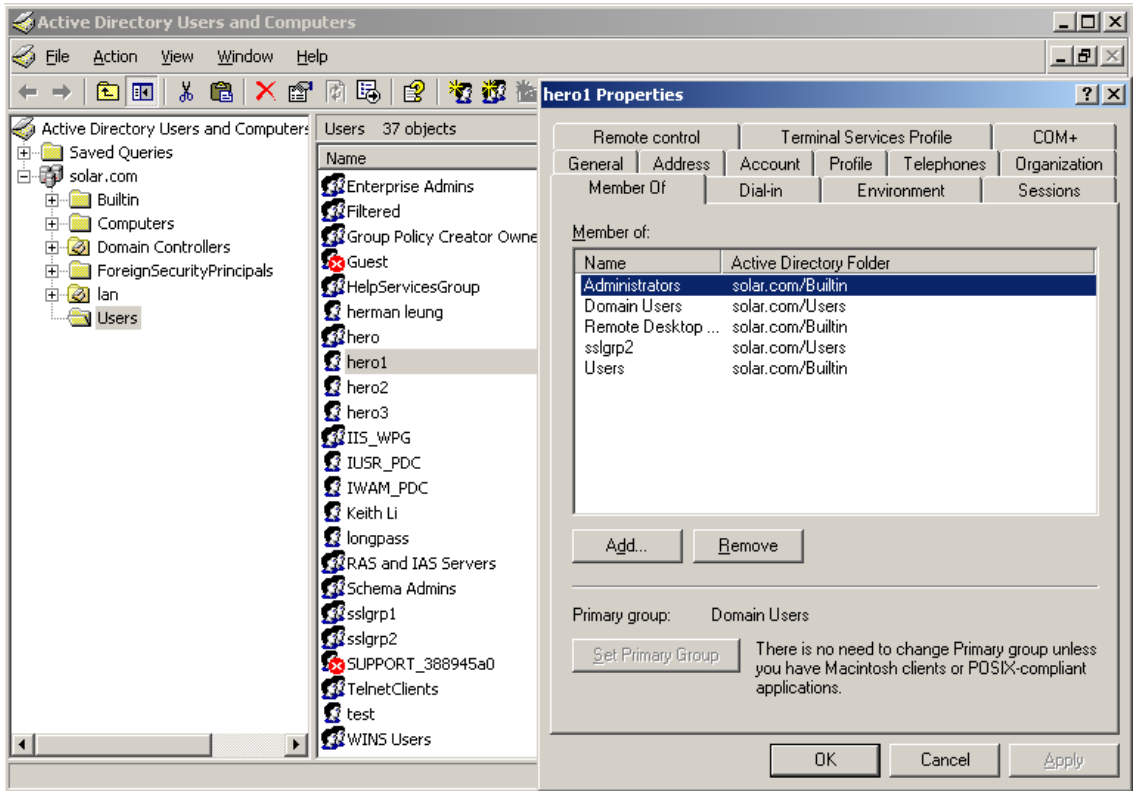
Step 5


sslgrp2 Properties
Settings
Specify the conditions that connection requests must match.
Policy conditions:
Windows-Groups matches "SOLAR\sslgrp2"
Add...
Edit...
Remove
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.
Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Specify additional connection attributes to be returned to the Remote Access server.
Attributes:
Name
Vendor
Value
Vendor-Specific
RADIUS Standard
sslgrp2, 172.16.87.88,
Configure VSA (RFC compliant)
Vendor-assigned attribute number:
1
Attribute format:
String
Attribute value:
sslgrp2
OK
Cancel
Multivalued Attribute Information
Attribute name:
Vendor-Specific
Attribute number:
26
Attribute format:
OctetString
Attribute values:
Vendor
Value
Vendor code: 12356
sslgrp2
Vendor code: 12356
172.16.87.88
Vendor code: 12356
root
Vendor code: 12356
Vendor code: 12356
wan1
Move Up
Move Down
Add
Remove
Edit
OK
Cancel
Vendor-Specific Attribute In
Attribute name:
Vendor-Specific
Specify network access server vendor.
Select from list:
Enter Vendor Code:
12356
Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.
Yes. It conforms.
No. It does not conform.
Configure Attribute...
OK
Cancel

Step 6


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
solar.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
lan
Users
Users 37 objects
Name
11pass
12pass
13pass
Administrator
blue1
blue2
Cert Publishers
DnsAdmins
DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Filtered
Group Policy Creator Owne
Guest
HelpServicesGroup
herman leung
hero
hero1
hero2
blue1 Properties
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Folder
Domain Users
solar.com/Users
sslgrp1
solar.com/Users
Users
solar.com/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply

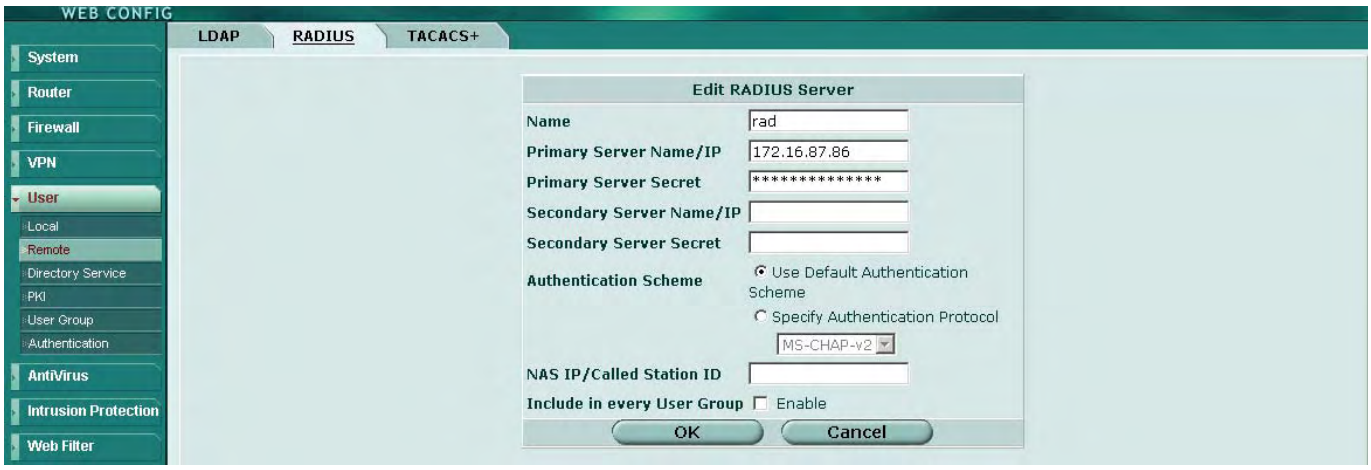
Step 7


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computers
Saved Queries
solar.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
lan
Users
Users 37 objects
Name
Enterprise Admins
Filtered
Group Policy Creator Owne
Guest
HelpServicesGroup
herman leung
hero
hero1
hero2
hero3
IIS_WPG
IUSR_PDC
IWAM_PDC
Keith Li
longpass
RAS and IAS Servers
Schema Admins
sslgrp1
sslgrp2
SUPPORT_388945a0
TelnetClients
test
WINS Users
hero1 Properties
Remote control
Terminal Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Folder
Administrators
solar.com/Builtin
Domain Users
solar.com/Users
Remote Desktop ...
solar.com/Builtin
sslgrp2
solar.com/Users
Users
solar.com/Builtin
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply

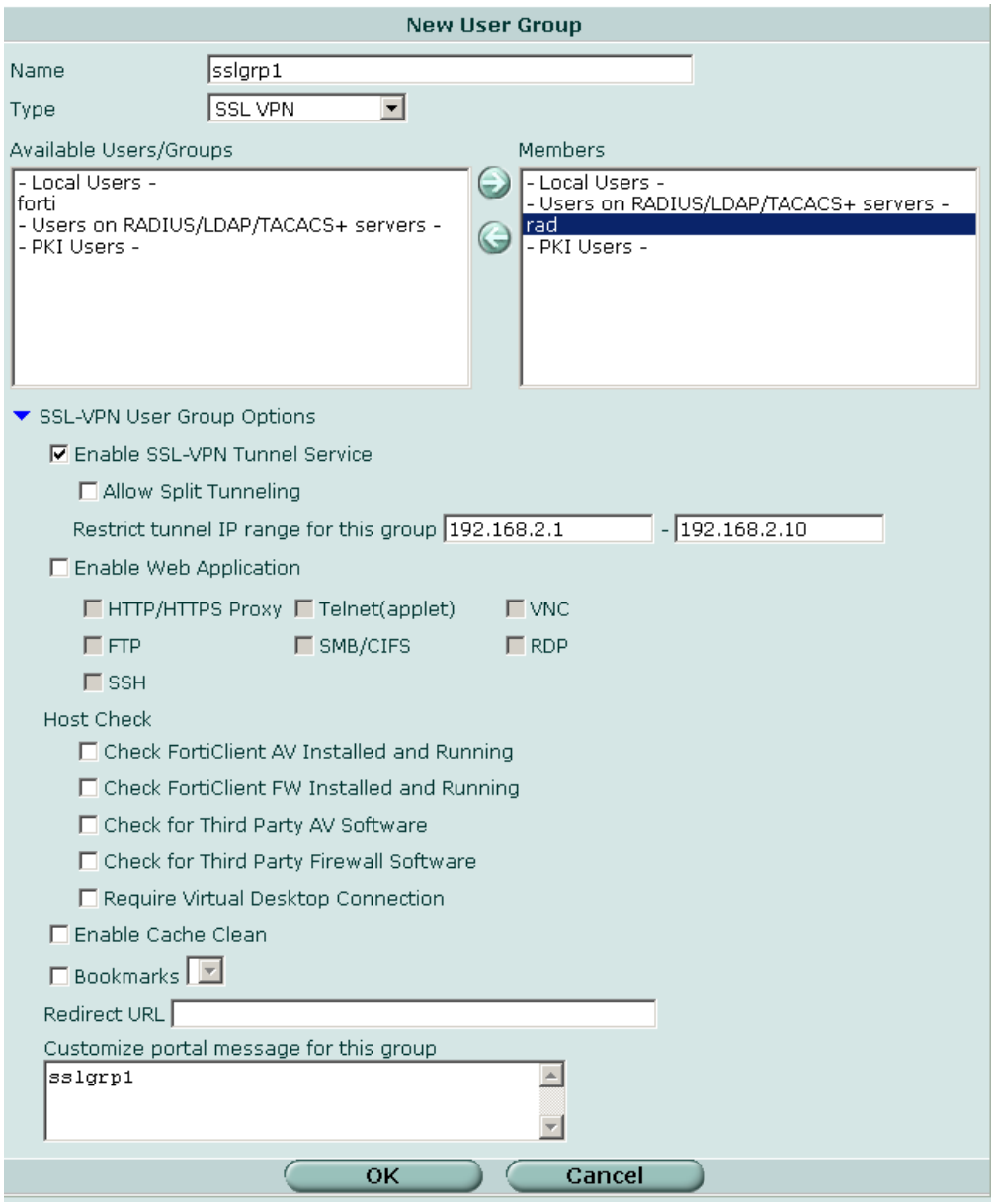
2. FortiGate configuration

Step 1

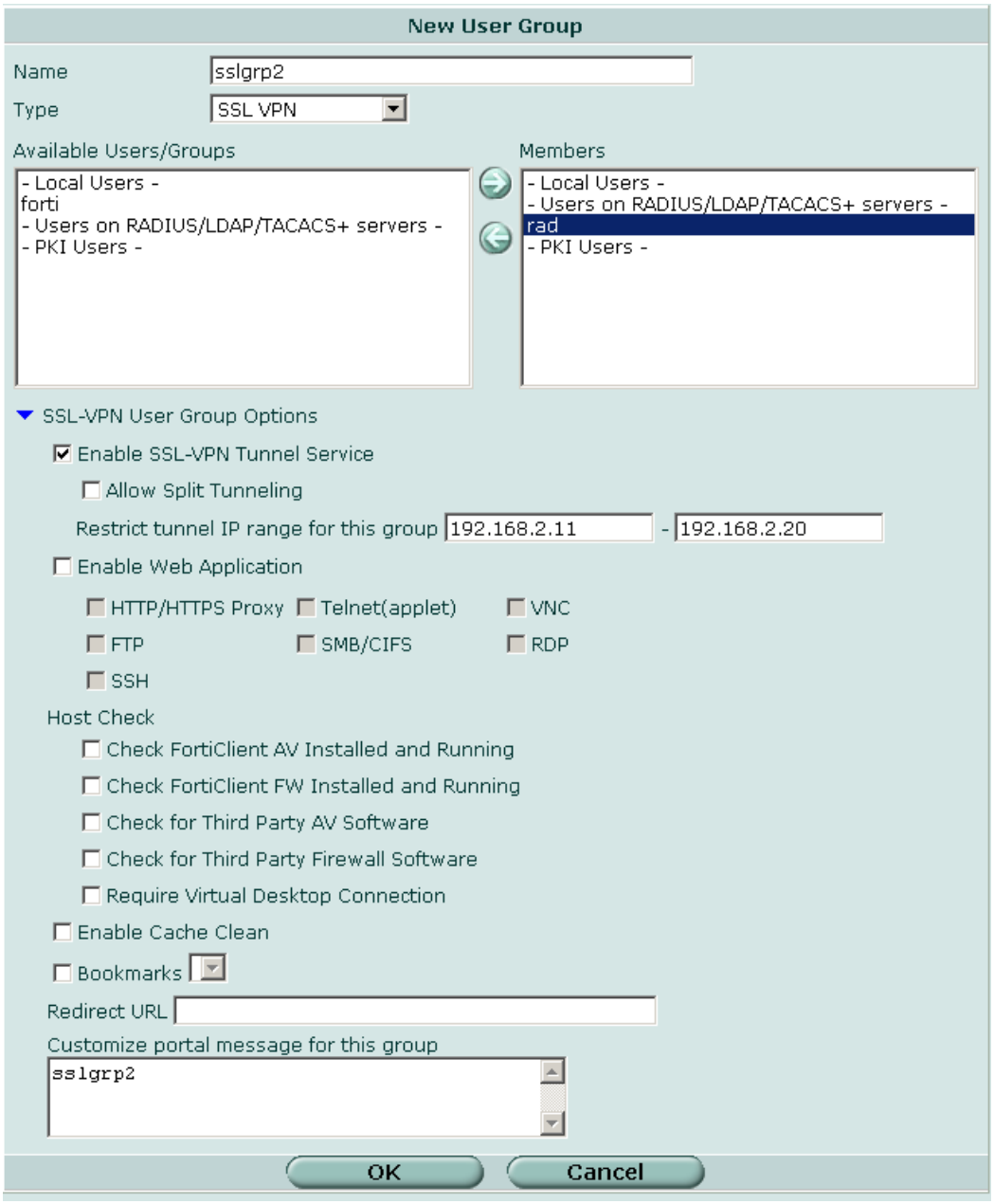
Step 2



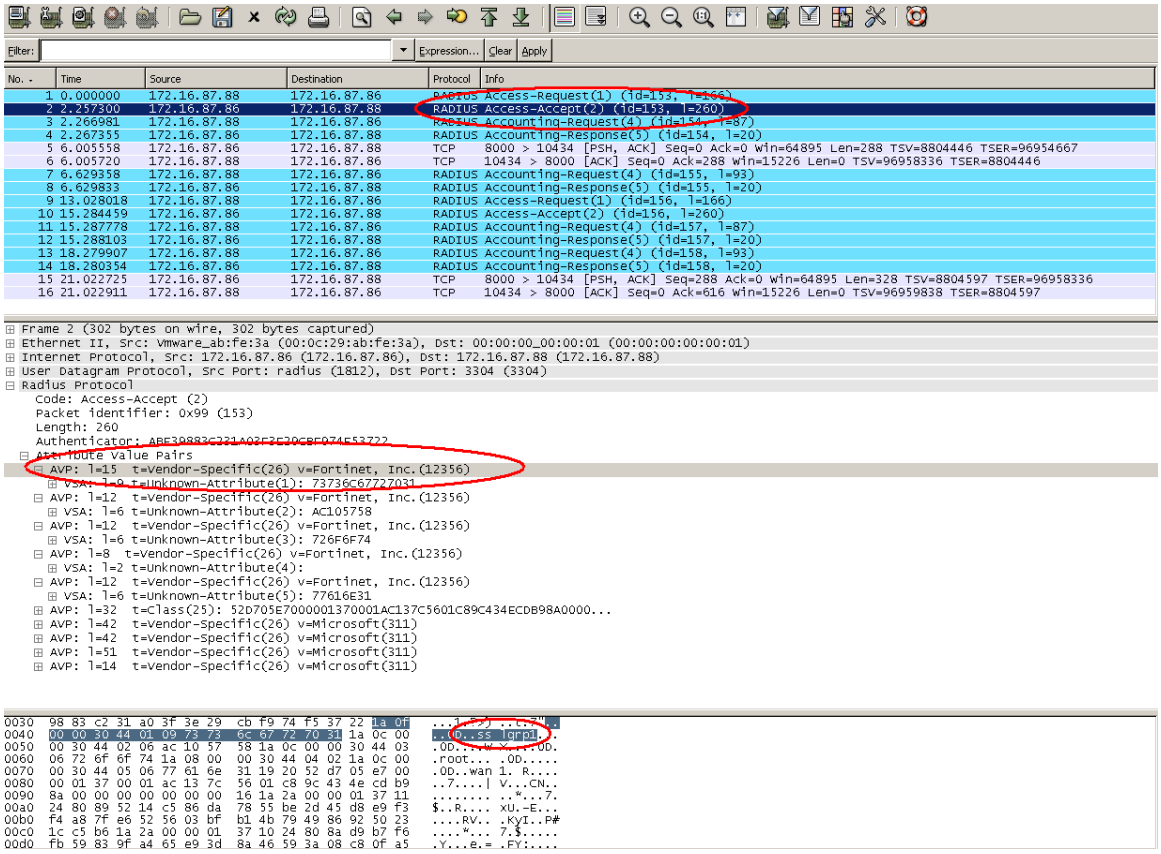
Step 3


New User Group
Name
sslgrp1
Type
SSL VPN
Available Users/Groups
- Local Users -
forti
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -
Members
- Local Users -
- Users on RADIUS/LDAP/TACACS+ servers -
rad
- PKI Users -
SSL-VPN User Group Options
Enable SSL-VPN Tunnel Service
Allow Split Tunneling
Restrict tunnel IP range for this group
192.168.2.1
192.168.2.10
Enable Web Application
HTTP/HTTPS Proxy
Telnet(applet)
VNC
FTP
SMB/CIFS
RDP
SSH
Host Check
Check FortiClient AV Installed and Running
Check FortiClient FW Installed and Running
Check for Third Party AV Software
Check for Third Party Firewall Software
Require Virtual Desktop Connection
Enable Cache Clean
Bookmarks
Redirect URL
Customize portal message for this group
sslgrp1
OK
Cancel

Step 4


New User Group
Name
sslgrp2
Type
SSL VPN
Available Users/Groups
- Local Users -
forti
- Users on RADIUS/LDAP/TACACS+ servers -
- PKI Users -
Members
- Local Users -
- Users on RADIUS/LDAP/TACACS+ servers -
rad
- PKI Users -
SSL-VPN User Group Options
Enable SSL-VPN Tunnel Service
Allow Split Tunneling
Restrict tunnel IP range for this group
192.168.2.11
-
192.168.2.20
Enable Web Application
HTTP/HTTPS Proxy
Telnet(applet)
VNC
FTP
SMB/CIFS
RDP
SSH
Host Check
Check FortiClient AV Installed and Running
Check FortiClient FW Installed and Running
Check for Third Party AV Software
Check for Third Party Firewall Software
Require Virtual Desktop Connection
Enable Cache Clean
Bookmarks
Redirect URL
Customize portal message for this group
sslgrp2
OK
Cancel

3. Example RADIUS packets



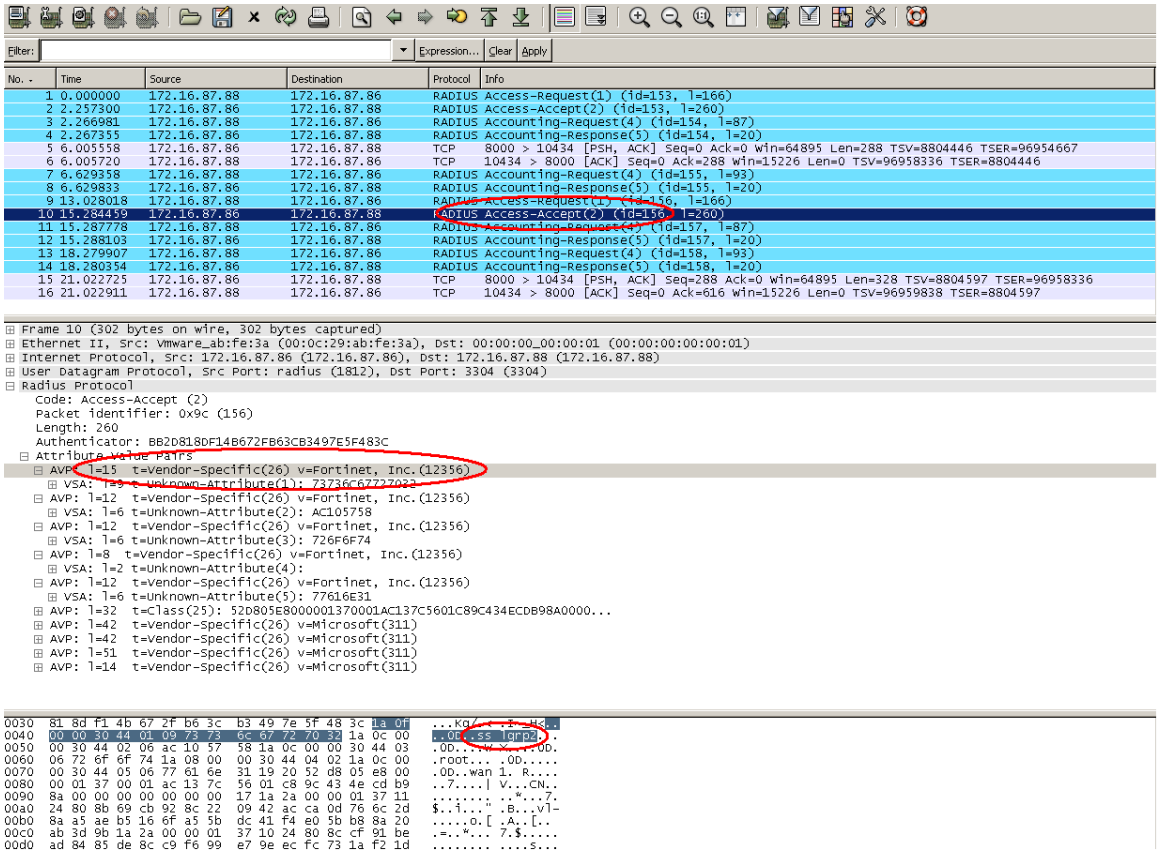
```
Filter:                                  Expression...  Clear  Apply

No. -  Time        Source           Destination      Protocol  Info
     1 0.000000    172.16.87.88     172.16.87.86     RADIUS    Access-Request(1) (id=153, l=166)
     2 2.257300    172.16.87.86     172.16.87.88     RADIUS    Access-Accept(2) (id=153, l=260)
     3 2.266981    172.16.87.88     172.16.87.86     RADIUS    Accounting-Request(4) (id=154, l=87)
     4 2.267355    172.16.87.86     172.16.87.88     RADIUS    Accounting-Response(5) (id=154, l=20)
     5 6.005558    172.16.87.86     172.16.87.88     TCP       8000 > 10434 [PSH, ACK] Seq=0 Ack=0 Win=64895 Len=288 TSV=8804446 TSER=96954667
     6 6.005720    172.16.87.86     172.16.87.88     TCP       10434 > 8000 [ACK] Seq=0 Ack=288 Win=15226 Len=0 TSV=96958336 TSER=8804446
     7 6.629358    172.16.87.88     172.16.87.86     RADIUS    Accounting-Request(4) (id=155, l=93)
     8 6.629833    172.16.87.86     172.16.87.88     RADIUS    Accounting-Response(5) (id=155, l=20)
     9 13.028018   172.16.87.88     172.16.87.86     RADIUS    Access-Request(1) (id=156, l=166)
    10 15.284459   172.16.87.86     172.16.87.88     RADIUS    Access-Accept(2) (id=156, l=260)
    11 15.287778   172.16.87.88     172.16.87.86     RADIUS    Accounting-Request(4) (id=157, l=87)
    12 15.288103   172.16.87.86     172.16.87.88     RADIUS    Accounting-Response(5) (id=157, l=20)
    13 18.279907   172.16.87.88     172.16.87.86     RADIUS    Accounting-Request(4) (id=158, l=93)
    14 18.280354   172.16.87.86     172.16.87.88     RADIUS    Accounting-Response(5) (id=158, l=20)
    15 21.022725   172.16.87.86     172.16.87.88     TCP       8000 > 10434 [PSH, ACK] Seq=288 Ack=0 Win=64895 Len=328 TSV=8804597 TSER=96958336
    16 21.022911   172.16.87.88     172.16.87.86     TCP       10434 > 8000 [ACK] Seq=0 Ack=616 Win=15226 Len=0 TSV=96959838 TSER=8804597

⊞ Frame 2 (302 bytes on wire, 302 bytes captured)
⊞ Ethernet II, Src: Vmware_ab:fe:3a (00:0c:29:ab:fe:3a), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
⊞ Internet Protocol, Src: 172.16.87.86 (172.16.87.86), Dst: 172.16.87.88 (172.16.87.88)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 3304 (3304)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x99 (153)
    Length: 260
    Authenticator: ABE39883C231A02F2E29CBF074E53722
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=15  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=9 t=Unknown-Attribute(1): 73736C67727031
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(2): AC105758
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(3): 726F6F74
    ⊟ AVP: l=8  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=2 t=Unknown-Attribute(4):
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(5): 77616E31
    ⊞ AVP: l=32  t=Class(25): 52D705E7000001370001AC137C5601C89C434ECDB98A0000...
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=14  t=Vendor-Specific(26) v=Microsoft(311)

0030  98 83 c2 31 a0 3f 3e 29  cb f9 74 f5 37 22 1a 0f   ...1.?>) ..t.7"..
0040  00 00 30 44 01 09 73 73  6c 67 72 70 31 1a 0c 00   ..0D..ss lgrp1...
0050  00 30 44 02 06 ac 10 57  58 1a 0c 00 00 30 44 03   .0D....W X....0D.
0060  06 72 6f 6f 74 1a 08 00  00 30 44 04 02 1a 0c 00   .root.... .0D.....
0070  00 30 44 05 06 77 61 6e  31 19 20 52 d7 05 e7 00   .0D..wan 1. R....
0080  00 01 37 00 01 ac 13 7c  56 01 c8 9c 43 4e cd b9   ..7....| V...CN..
0090  8a 00 00 00 00 00 00 00  16 1a 2a 00 00 01 37 11   ........ ..*...7.
00a0  24 80 89 52 14 c5 86 da  78 55 be 2d 45 d8 e9 f3   $..R.... xU.-E...
00b0  f4 a8 7f e6 52 56 03 bf  b1 4b 79 49 86 92 50 23   ....RV.. .KyI..P#
00c0  1c c5 b6 1a 2a 00 00 01  37 10 24 80 8a d9 b7 f6   ....*... 7.$.....
00d0  fb 59 83 9f a4 65 e9 3d  8a 46 59 3a 08 c8 0f a5   .Y...e.= .FY:....
```

3. Example RADIUS packets (continued)



Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.87.88	172.16.87.86	RADIUS	Access-Request(1) (id=153, l=166)
2	2.257300	172.16.87.86	172.16.87.88	RADIUS	Access-Accept(2) (id=153, l=260)
3	2.266981	172.16.87.88	172.16.87.86	RADIUS	Accounting-Request(4) (id=154, l=87)
4	2.267355	172.16.87.86	172.16.87.88	RADIUS	Accounting-Response(5) (id=154, l=20)
5	6.005558	172.16.87.86	172.16.87.88	TCP	8000 > 10434 [PSH, ACK] Seq=0 Ack=0 Win=64895 Len=288 TSV=8804446 TSER=96954667
6	6.005720	172.16.87.88	172.16.87.86	TCP	10434 > 8000 [ACK] Seq=0 Ack=288 Win=15226 Len=0 TSV=96958336 TSER=8804446
7	6.629358	172.16.87.88	172.16.87.86	RADIUS	Accounting-Request(4) (id=155, l=93)
8	6.629833	172.16.87.86	172.16.87.88	RADIUS	Accounting-Response(5) (id=155, l=20)
9	13.028018	172.16.87.88	172.16.87.86	RADIUS	Access-Request(1) (id=156, l=166)
10	15.284459	172.16.87.86	172.16.87.88	RADIUS	Access-Accept(2) (id=156, l=260)
11	15.287778	172.16.87.88	172.16.87.86	RADIUS	Accounting-Request(4) (id=157, l=87)
12	15.288103	172.16.87.86	172.16.87.88	RADIUS	Accounting-Response(5) (id=157, l=20)
13	18.279907	172.16.87.88	172.16.87.86	RADIUS	Accounting-Request(4) (id=158, l=93)
14	18.280354	172.16.87.86	172.16.87.88	RADIUS	Accounting-Response(5) (id=158, l=20)
15	21.022725	172.16.87.86	172.16.87.88	TCP	8000 > 10434 [PSH, ACK] Seq=288 Ack=0 Win=64895 Len=328 TSV=8804597 TSER=96958336
16	21.022911	172.16.87.88	172.16.87.86	TCP	10434 > 8000 [ACK] Seq=0 Ack=616 Win=15226 Len=0 TSV=96959838 TSER=8804597

```
⊞ Frame 10 (302 bytes on wire, 302 bytes captured)
⊞ Ethernet II, Src: Vmware_ab:fe:3a (00:0c:29:ab:fe:3a), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
⊞ Internet Protocol, Src: 172.16.87.86 (172.16.87.86), Dst: 172.16.87.88 (172.16.87.88)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 3304 (3304)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x9c (156)
    Length: 260
    Authenticator: BB2D818DF14B672FB63CB3497E5F483C
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=15  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=9 t=Unknown-Attribute(1): 73736C67727023
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(2): AC105758
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(3): 726F6F74
    ⊟ AVP: l=8  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=2 t=Unknown-Attribute(4):
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet, Inc.(12356)
      ⊞ VSA: l=6 t=Unknown-Attribute(5): 77616E31
    ⊞ AVP: l=32  t=Class(25): 52D805E800000137000 1AC137C5601C89C434ECDB98A0000...
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=14  t=Vendor-Specific(26) v=Microsoft(311)
```

```
0030  81 8d f1 4b 67 2f b6 3c  b3 49 7e 5f 48 3c 1a 0f   ...Kg/.< .I~_H<..
0040  00 00 30 44 01 09 73 73  6c 67 72 70 32 1a 0c 00   ..0D..ss lgrp2...
0050  00 30 44 02 06 ac 10 57  58 1a 0c 00 00 30 44 03   .0D....W X....0D.
0060  06 72 6f 6f 74 1a 08 00  00 30 44 04 02 1a 0c 00   .root.... .0D.....
0070  00 30 44 05 06 77 61 6e  31 19 20 52 d8 05 e8 00   .0D..wan 1. R.....
0080  00 01 37 00 01 ac 13 7c  56 01 c8 9c 43 4e cd b9   ..7....| V...CN..
0090  8a 00 00 00 00 00 00 00  17 1a 2a 00 00 01 37 11   ........ ..*...7.
00a0  24 80 8b 69 cb 92 8c 22  09 42 ac ca 0d 76 6c 2d   $..i..." .B...vl-
00b0  8a a5 ae b5 16 6f a5 5b  dc 41 f4 e0 5b b8 8a 20   .....o.[ .A..[..
00c0  ab 3d 9b 1a 2a 00 00 01  37 10 24 80 8c cf 91 be   .=..*... 7.$.....
00d0  ad 84 85 de 8c c9 f6 99  e7 9e ec fc 73 1a f2 1d   ........ ....s...
```