Configure a Client-to-Site VPN Using L2TP over IPsec (Routing Mode)

Lab 4

Objectives

After completing this lab, you should be able to configure the Threat Management Services (TMS) zl Module to support client-to-site Virtual Private Networks (VPNs):

- Create a user group
- Configure an Internet Key Exchange (IKEv1) policy
- Configure an IP security (IPsec) proposal
- Configure an IPsec policy
- Configure a Layer 2 Tunneling Protocol (L2TP) policy
- Create L2TP Dial-in users
- Configure a Windows client to establish a VPN with the TMS zl Module
- Establish a client-to-site VPN using L2TP over IP Security (IPsec)

Requirements

For this lab, you and your partner will need:

- One HP ProCurve Series 5400zl switch
  - Software version K.13.51 or above

Note

You can substitute an HP ProCurve 8212zl switch, but it must run the same software version—version K.13.51 or above. To configure the 8212zl switch through a serial connection, you will need an RJ-45 to DB-9 adapter cable (5188-3836).

- One HP ProCurve Threat Management Services zl Module
  - Services operating system (OS) version 1.0.081219 or above
  - TMS OS version ST 1.0.090116 or above
- One serial cable (5184-1894)
- Three 1-meter CAT5e cables

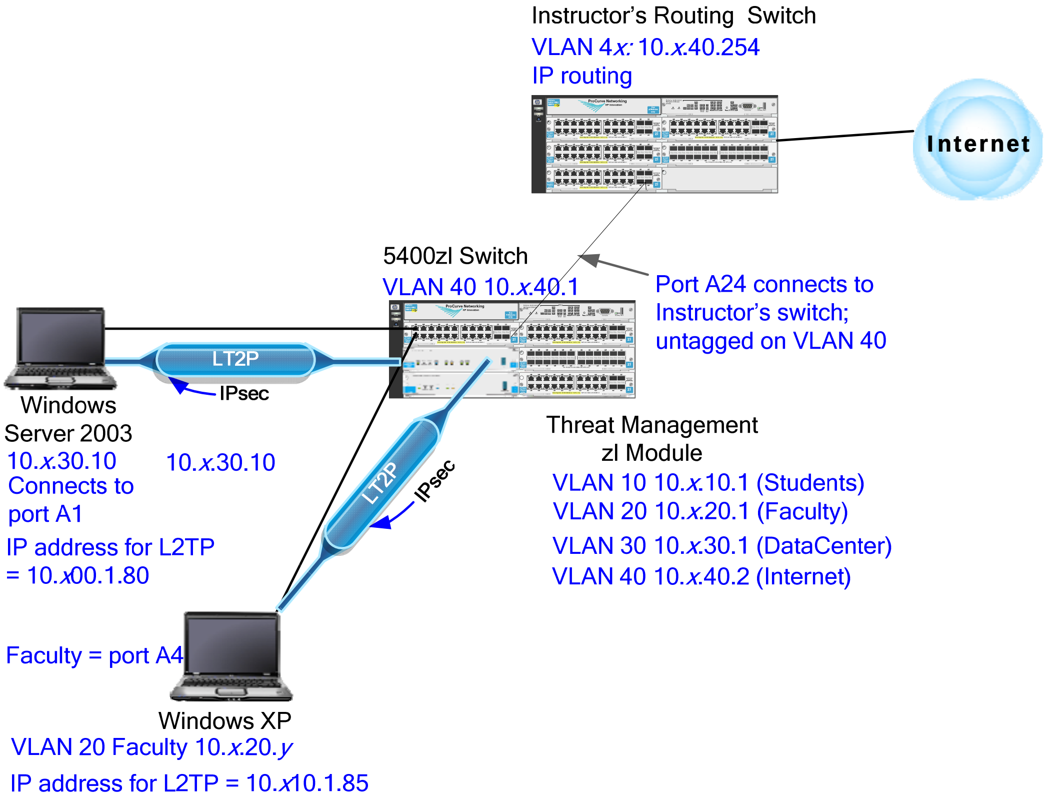
- Windows Server 2003 with the following components:
  - DHCP services
  - Windows Remote Desktop Program (RDP)
  - Microsoft Internet Explorer 7.0 or above with support for Java applets or another Web browser that supports Java applets
  - Console terminal software such as Tera Term
  - Wireshark for Windows 2000/XP/2003/Vista/2008
- One Microsoft Windows XP Professional Workstation
  - Windows XP Service Pack (SP) 2
  - Microsoft Internet Explorer 7.0 or above with support for Java applets or another Web browser that supports Java applets
  - TFTP server such as Tftpd32
  - Console terminal software such as Tera Term

Purpose

ProCurve University (PCU) administration has decided that information on certain servers in the data center is so sensitive that all transmission of this information must be encrypted. The IT staff will use the TMS zl Module to establish an L2TP over IPsec client-to-site VPN to protect this information. Data center servers will log in to this VPN as will faculty users who are allowed to access the sensitive data.

Network Diagram

After you complete this lab activity, your network’s topology and IP addressing should resemble the diagram below.


Instructor’s Routing Switch
VLAN 4x: 10.x.40.254
IP routing
Internet
5400zl Switch
VLAN 40 10.x.40.1
Port A24 connects to Instructor’s switch; untagged on VLAN 40
LT2P
IPsec
Windows Server 2003
10.x.30.10
Connects to port A1
10.x.30.10
IP address for L2TP = 10.x00.1.80
LT2P
IPsec
Threat Management zl Module
VLAN 10 10.x.10.1 (Students)
VLAN 20 10.x.20.1 (Faculty)
VLAN 30 10.x.30.1 (DataCenter)
VLAN 40 10.x.40.2 (Internet)
Faculty = port A4
Windows XP
VLAN 20 Faculty 10.x.20.y
IP address for L2TP = 10.x10.1.85

Special Instructions

In these TMS zl Module labs, you will work with a partner.

Several programs are installed on your workstations to help you configure, manage, and troubleshoot your infrastructure devices:

- Tera Term, a terminal emulation program
- Tftp32, a TFTP server program that is used to back up and restore configurations and download software images
- Web browser
- Wireshark

Devices in this lab should use the following IP addresses.

Device	IP Address	Subnet Mask
5400zl switch	VLAN 40 10.*x*.40.1	255.255.255.0
Windows XP Professional	10.*x*.20.*y* (dynamic IP address)	255.255.255.0
Windows Server 2003	10.*x*.30.10	255.255.255.0

You can substitute a ProCurve 8212zl Switch for the 5400zl switch.

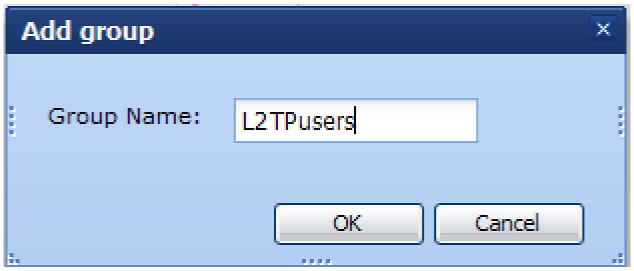
The TMS zl Module should have the following VLANs and IP addresses.

VLAN ID	Zone	IP Address	Description
10	Internal	10.*x*.10.1	Students
20	Internal	10.*x*.20.1	Faculty
30	Zone1	10.*x*.30.1	Data Center
40	External	10.*x*.40.2	Internet

Task 1: Create a User Group for L2TP Users

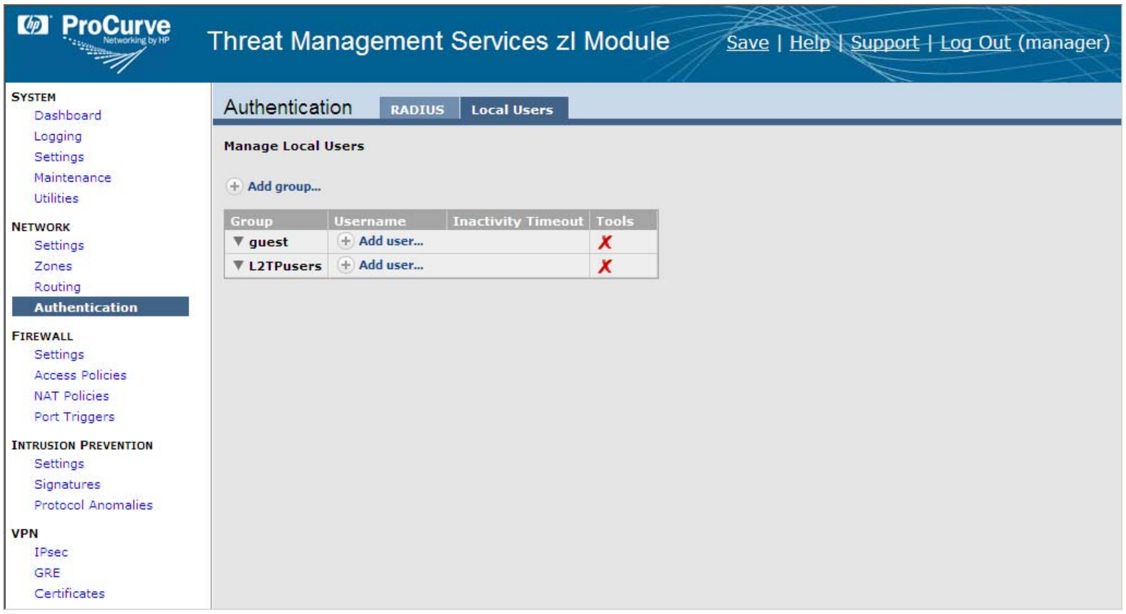
In this task, you will configure a user group for the users who will be logging in to the network using the L2TP over IPsec client-to-site VPN.

1. Select ***Network*** > ***Authentication*** and click the ***Local Users*** tab.
2. Click ***Add group***.
3. For ***Group Name***, type ***L2TPusers***.



Group Name: L2TPusers

4. Click ***OK***.



Group	Username	Inactivity Timeout	Tools
▼ guest	+ Add user...		✗
▼ L2TPusers	+ Add user...		✗

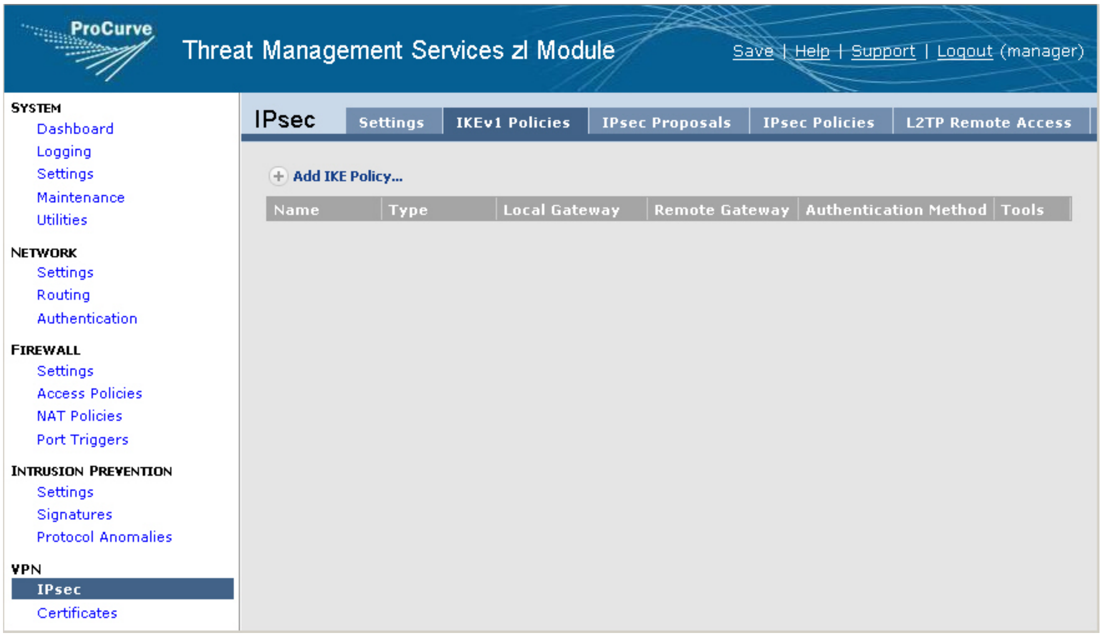
Task 2: Configure an IKEv1 Policy

In this task, you will configure the IKEv1 policy that the TMS zl Module will use to negotiate the client-to-site VPN with the VPN clients on data servers and faculty workstations.

You will use the following parameters to configure your IKEv1 policy.

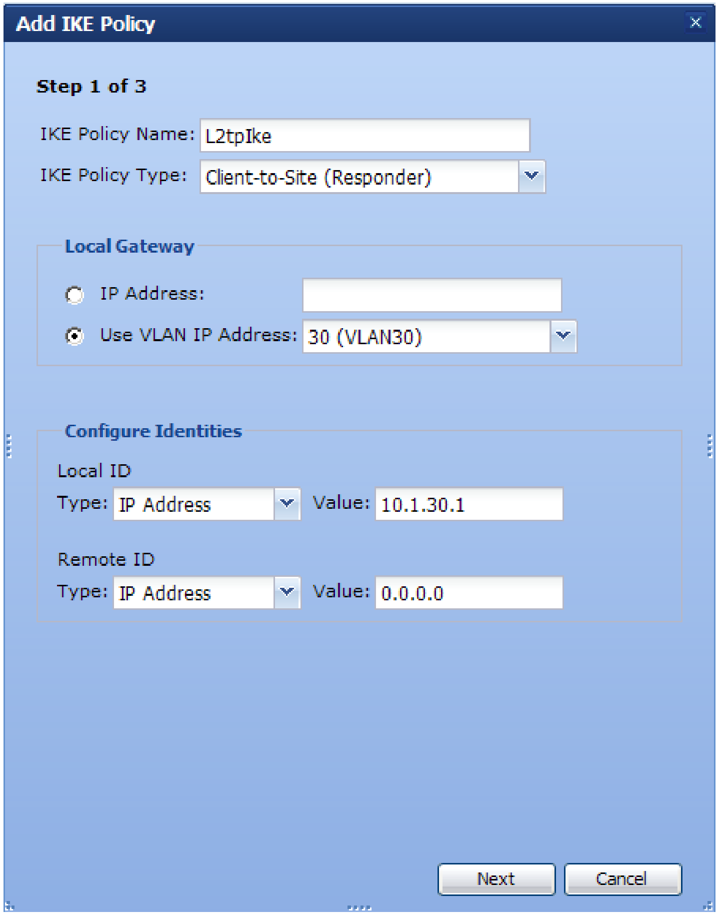
Parameter	Setting
Type of policy	Client-to-Site (Responder)
Local gateway	VLAN 30
Local ID	IP address—10.*x*.30.1
Remote ID	IP address—0.0.0.0
Key exchange mode	Main
Authentication method	Pre-shared key—procurvetestvpn
Diffie-Hellman group	Group 2 (1024)
Encryption algorithm (Encrypt alg)	3DES
Authentication algorithm (Hash alg)	MD5
SA lifetime (SA life)	28800

1. Select ***VPN*** > ***IPsec***. Then click the ***IKEv1 Policies*** tab.



2. Click ***Add IKE Policy***.
3. For ***IKE Policy Name***, type ***L2tpIke***.
4. For ***IKE Policy Type***, select ***Client-to-Site (Responder)***.
5. For ***Local Gateway***, select ***Use VLAN IP Address*** and select ***30 (VLAN30)*** from the list. This sets the IP address 10.*x*.30.1 as the local gateway address.
6. For ***Local ID***, configure the ID that the TMS zl Module sends to authenticate itself. From the ***Type*** list, select ***IP Address***, and type ***10.x.30.1*** in the box provided.

7. For ***Remote ID***, specify the ID that the remote workstation sends to authenticate itself. From the ***Type*** list, select ***IP Address***, and type ***0.0.0.0*** in the value field provided.



Add IKE Policy

Step 1 of 3

IKE Policy Name: L2tpIke

IKE Policy Type: Client-to-Site (Responder)

Local Gateway

○ IP Address:

● Use VLAN IP Address: 30 (VLAN30)

Configure Identities

Local ID

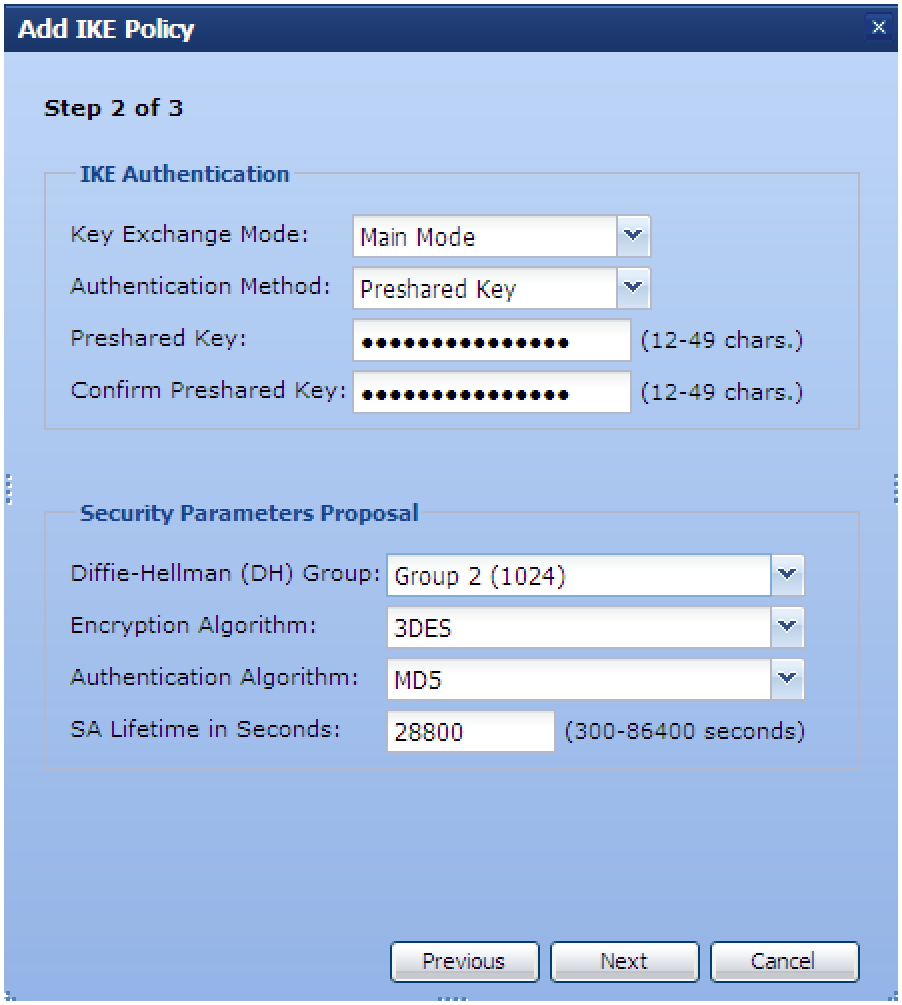
Type: IP Address Value: 10.1.30.1

Remote ID

Type: IP Address Value: 0.0.0.0

8. Click ***Next***.
9. Configure ***IKE Authentication***:
   a. For ***Key Exchange Mode***, select ***Main Mode***.
   b. For ***Authentication Method***, select ***Preshared Key***.
   c. For ***Preshared Key*** and ***Confirm Preshared Key***, type ***procurvetestvpn***.
10. Configure ***Security Parameters Proposal***:
    a. For Diffie-Hellman (DH) Group, select ***Group 2 (1024)***.
    b. For ***Encryption Algorithm***, accept the default: ***3DES***.
    c. For ***Authentication Algorithm***, accept the default: ***MD5***.

d. For ***SA Lifetime in seconds***, accept the default: ***28800***.



Add IKE Policy

Step 2 of 3

IKE Authentication

Key Exchange Mode: Main Mode

Authentication Method: Preshared Key

Preshared Key: ••••••••••••••• (12-49 chars.)

Confirm Preshared Key: ••••••••••••••• (12-49 chars.)

Security Parameters Proposal

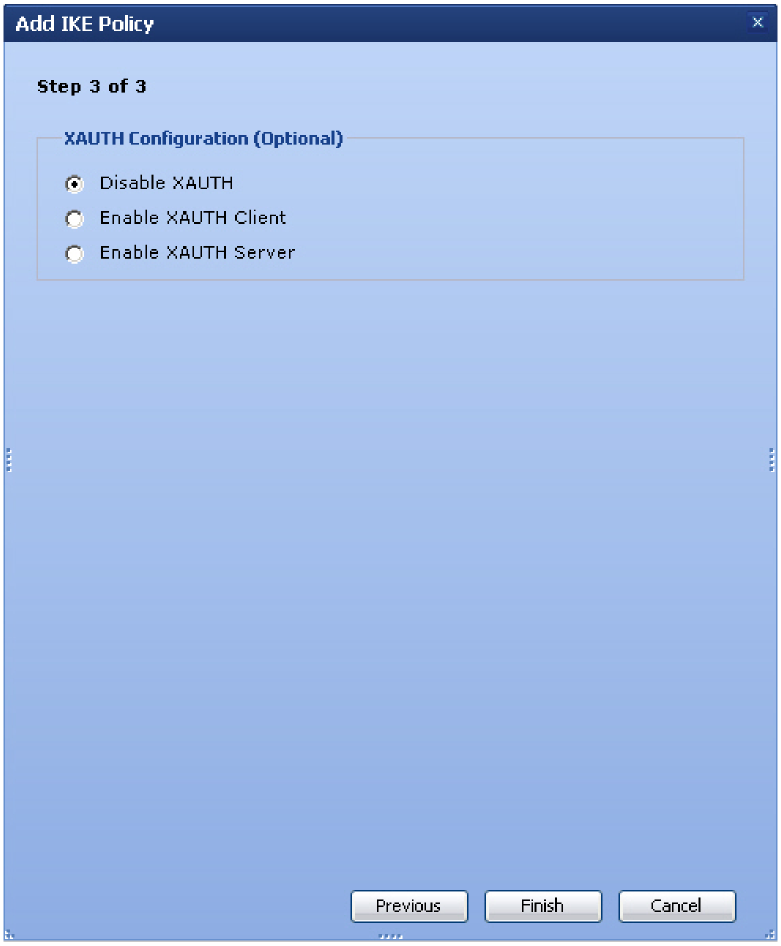
Diffie-Hellman (DH) Group: Group 2 (1024)

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

SA Lifetime in Seconds: 28800 (300-86400 seconds)

11. Click ***Next***.
12. Under ***XAUTH Configuration (Optional)***, select ***Disable XAUTH***.



Step 3 of 3

XAUTH Configuration (Optional)

● Disable XAUTH

○ Enable XAUTH Client

○ Enable XAUTH Server

13. Click ***Finish***.

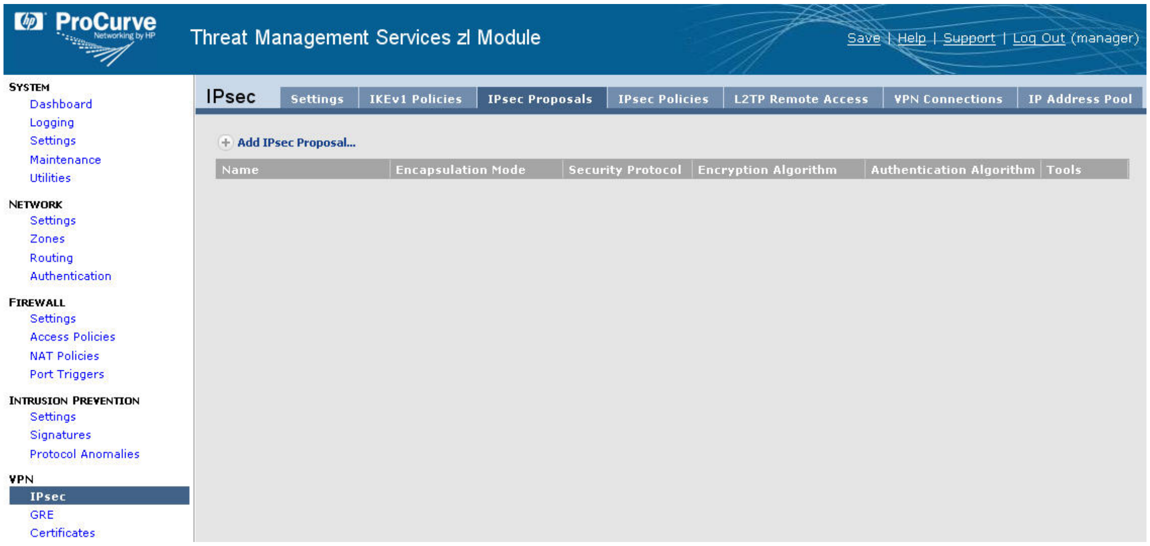
Task 3: Configure an IPsec Proposal

In this task, you will configure the algorithms that will secure traffic sent across the VPN.

You will use the following parameters to configure your IPsec proposal.

Parameter	Setting
Encapsulation mode	Transport mode
Security protocol	ESP
Encryption algorithm	3DES
Authentication algorithm	MD5

1. From the ***VPN*** > ***IPsec*** > ***IKEv1 Policies*** window, click the ***IPsec Proposals*** tab.



Name	Encapsulation Mode	Security Protocol	Encryption Algorithm	Authentication Algorithm	Tools

2. Click ***Add IPsec Proposal***.

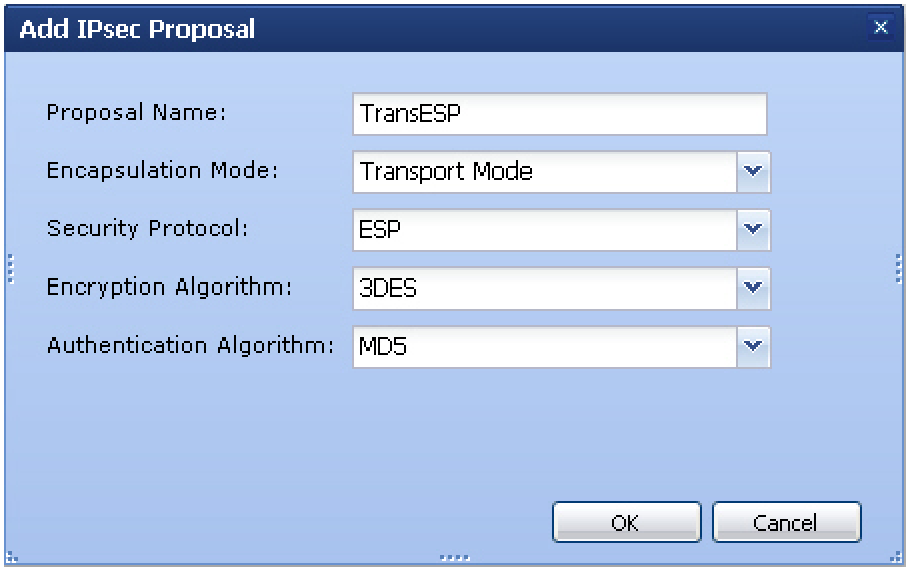
3. For ***Proposal Name***, type ***TransESP***.

4. For ***Encapsulation Mode***, select ***Transport Mode***.

5. For ***Security Protocol***, accept the default: ***ESP***.

6. For ***Encryption Algorithm***, accept the default: ***3DES***.

7. For ***Authentication Algorithm***, accept the default: ***MD5***.



Add IPsec Proposal

Proposal Name: TransESP

Encapsulation Mode: Transport Mode

Security Protocol: ESP

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

8. Click ***OK***.

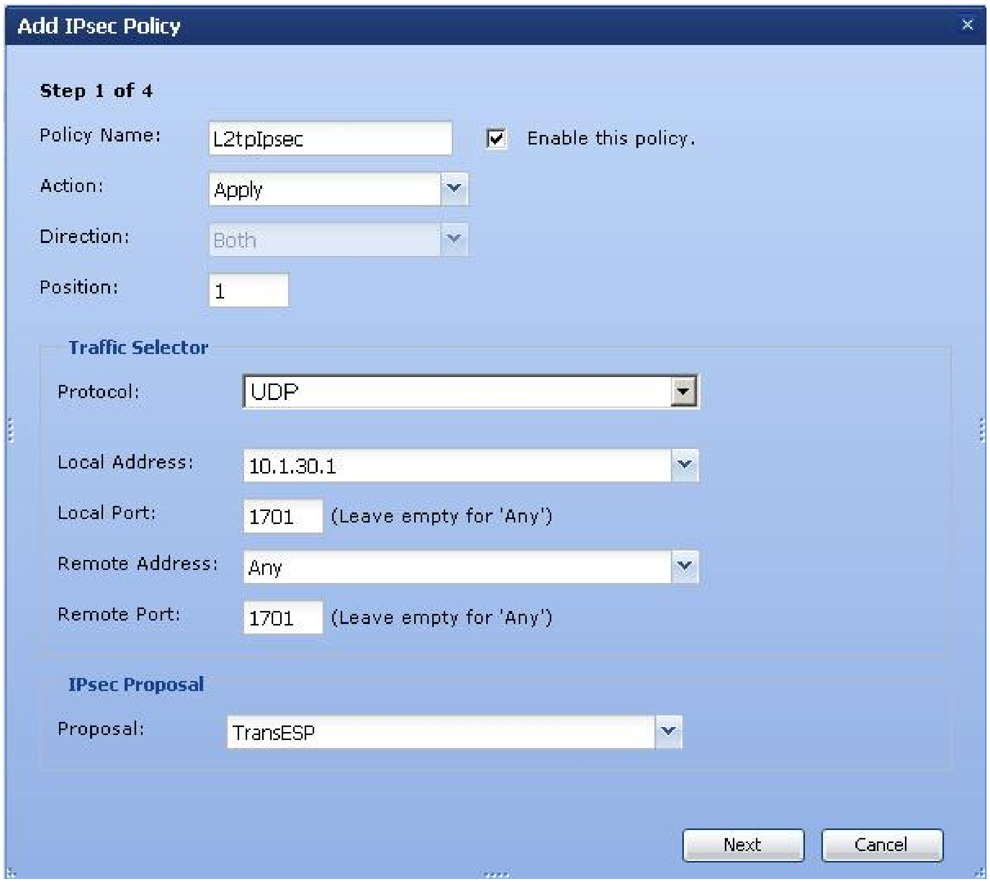
Task 4: Configure an IPsec Policy for L2TP Users

In this task, you will configure the settings for the IPsec SA, which selects all traffic sent on L2TP connections for encryption.

You will use the following parameters to configure your IPsec Policy.

Parameter	**Setting**
Protocol	UDP
Local address	10.*x*.30.1
Local port	1701
Remote address	Any
Remote port	1701
IKE exchange method	Auto
IPsec proposal	TransESP
IKEv1 policy	L2tpIke
Perfect Forward Secrecy	Disabled
SA lifetime in seconds (SA life)	28800
SA lifetime in kilobytes	0
Mode config address pool	Disabled

1. From the ***VPN*** > ***IPsec*** > ***IKEv1 Policies*** window, click the ***IPsec Policies*** tab.
2. Click ***Add IPsec Policy***.
3. For ***Policy Name***, type ***L2tpIpsec***.
4. Ensure that the ***Enable this policy*** check box is selected.
5. For ***Action***, accept the default: ***Apply***.
6. For ***Position***, accept the default: ***1***.
7. Configure the ***Traffic Selector***:
   a. For ***Protocol***, select ***UDP***.
   b. For ***Local Address***, type ***10.x.30.1***.
   c. For ***Local Port***, type ***1701***.
   d. For ***Remote Address***, select ***Any***.
   e. For ***Remote Port***, type ***1701***.
8. Under ***IPsec Proposal***, for ***Proposal***, select the proposal that you created in task 3: ***TransESP***.



Add IPsec Policy

Step 1 of 4

Policy Name: L2tpIpsec ☑ Enable this policy.

Action: Apply

Direction: Both

Position: 1

Traffic Selector

Protocol: UDP

Local Address: 10.1.30.1

Local Port: 1701 (Leave empty for 'Any')

Remote Address: Any

Remote Port: 1701 (Leave empty for 'Any')

IPsec Proposal

Proposal: TransESP

9. Click ***Next***.

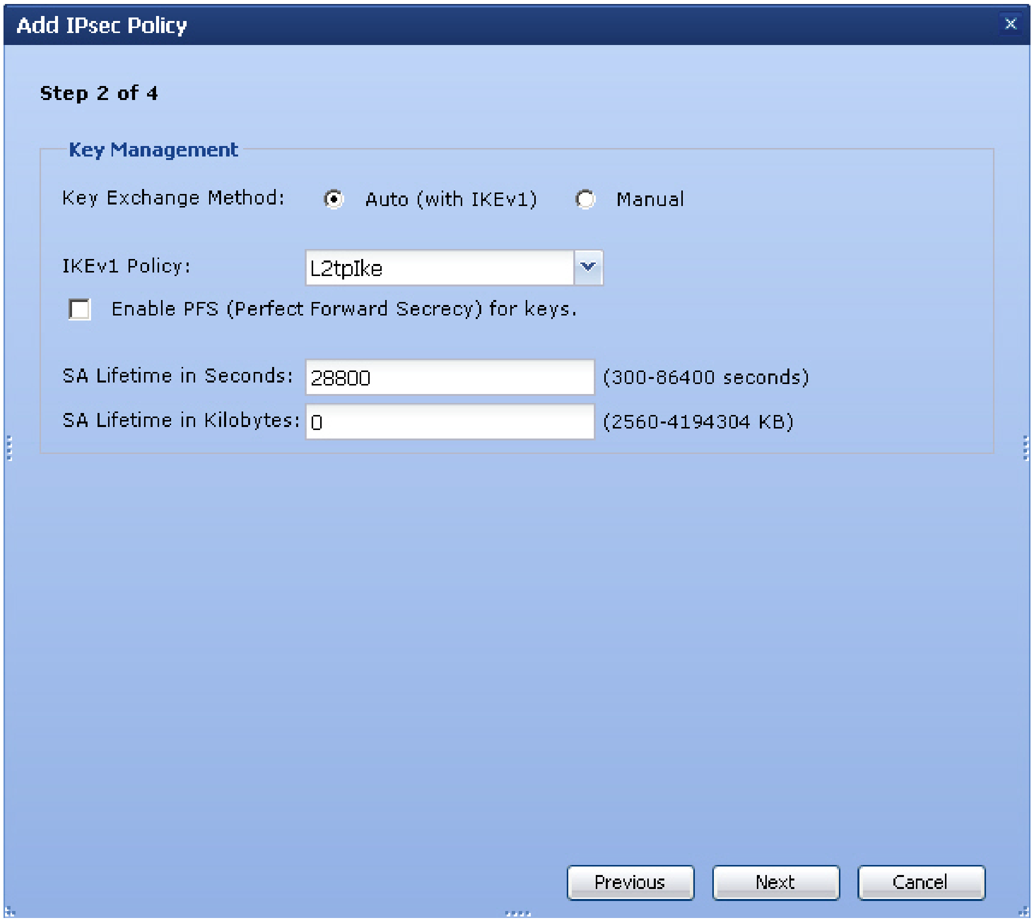
10. Under ***Key Management***, for ***Key Exchange Method***, accept the default: ***Auto (with IKEv1)***.

11. For ***IKEv1 Policy***, select the IKEv1 policy that you created in task 2, ***L2tpIke***.

12. Leave the ***Enable PFS (Perfect Forward Secrecy) for keys*** check box cleared.

13. For ***SA Lifetime in Seconds***, leave the default setting (***28800***).

14. For ***SA Lifetime in Kilobytes***, leave the default setting (***0***).



Add IPsec Policy

Step 2 of 4

Key Management

Key Exchange Method: ● Auto (with IKEv1) ○ Manual

IKEv1 Policy: L2tpIke

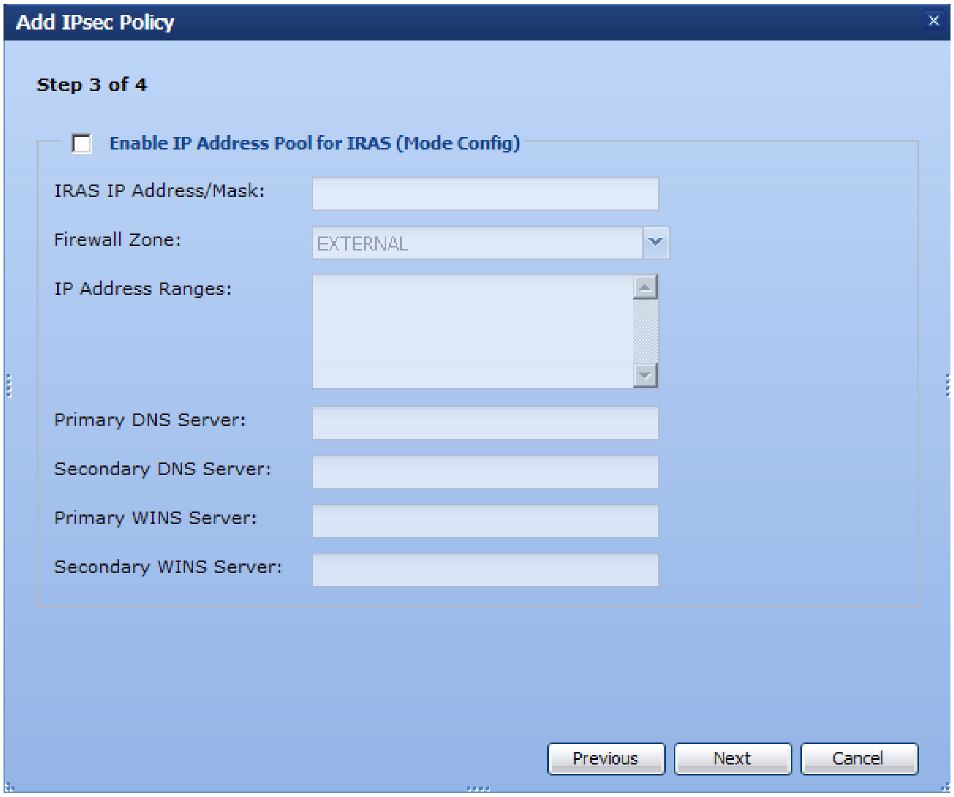
□ Enable PFS (Perfect Forward Secrecy) for keys.

SA Lifetime in Seconds: 28800 (300-86400 seconds)

SA Lifetime in Kilobytes: 0 (2560-4194304 KB)

15. Click ***Next***.

16. Clear the ***Enable IP Address Pool for IRAS (Mode Config)*** check box.
17. Leave all other fields blank.



Step 3 of 4

☐ Enable IP Address Pool for IRAS (Mode Config)

IRAS IP Address/Mask:

Firewall Zone: EXTERNAL

IP Address Ranges:

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

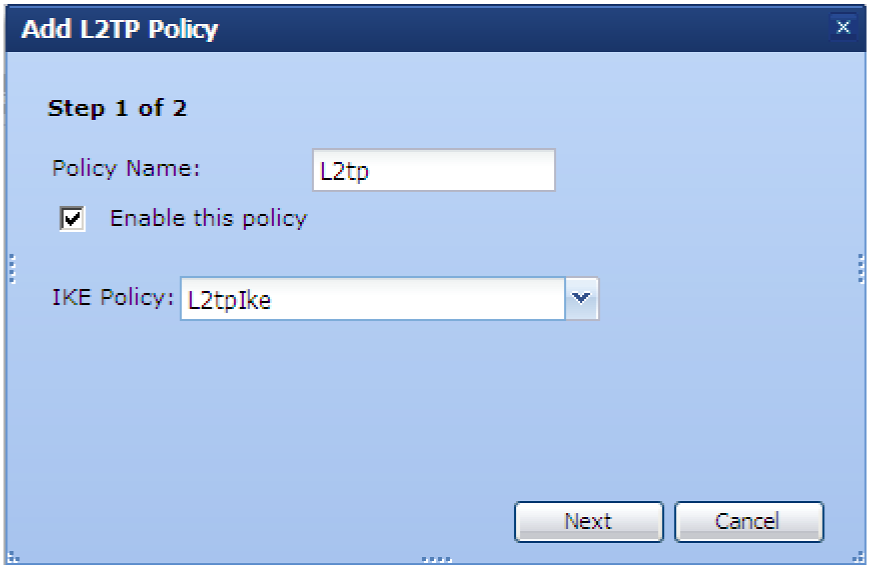
18. Click ***Next***.
19. Accept the default settings and click ***Finish***.

Task 5: Configure an L2TP Policy

You will use the following parameters to configure your L2TP Policy.

Parameter	**Setting**
IKEv1 policy	L2tpIke
IPsec proposal	TransESP
SA lifetime	28800

1. From the ***VPN*** > ***IPsec*** > ***IPsec Policies*** window, click the ***L2TP Remote Access*** tab.
2. Click ***Add L2TP Policy***.
3. For ***Policy Name***, type ***L2tp***.
4. Select the ***Enable this policy*** check box.
5. For ***IKE Policy***, select the policy you created in task 2, ***L2tpIke***.



Add L2TP Policy

Step 1 of 2

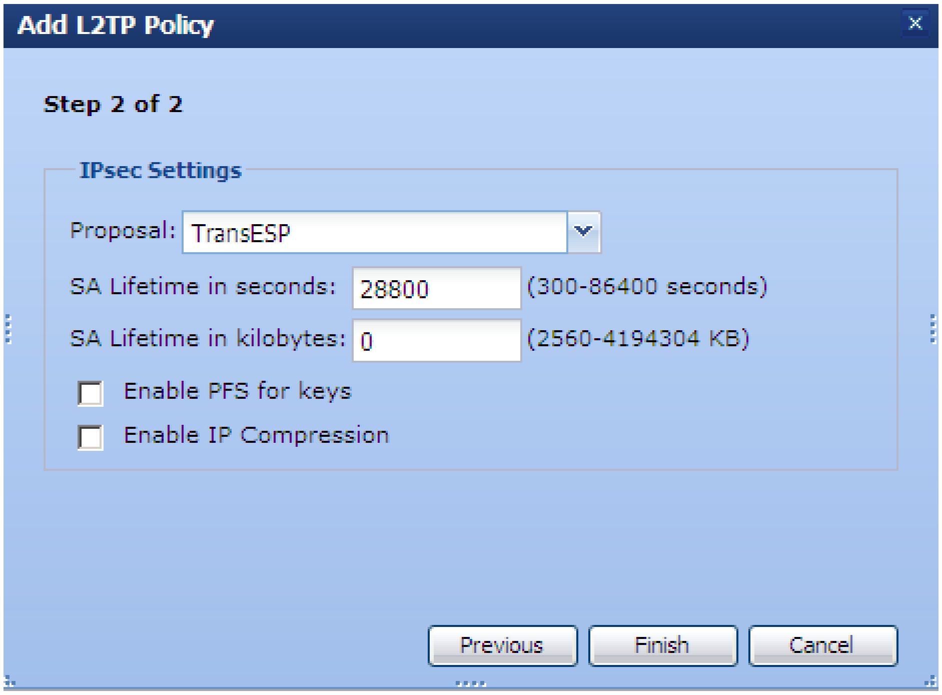
Policy Name: L2tp

☑ Enable this policy

IKE Policy: L2tpIke

6. Click ***Next***.

7. For ***Proposal***, select the proposal you created in task 3, ***TransESP***.
8. For ***SA Lifetime in seconds***, accept the default setting (***28800***).
9. For ***SA Lifetime in kilobytes***, accept the default setting (***0***).



Proposal: TransESP

SA Lifetime in seconds: 28800 (300-86400 seconds)

SA Lifetime in kilobytes: 0 (2560-4194304 KB)

□ Enable PFS for keys

□ Enable IP Compression

10. Click ***Finish***.

Task 6: Add L2TP Dial-in Users

The TMS zl Module requires a separate dial-in user account for each server and for each faculty member who will log in to the L2TP over IPsec VPN.

In this lab, you will create one account for a data server and one account for a faculty member. Use the following parameters.

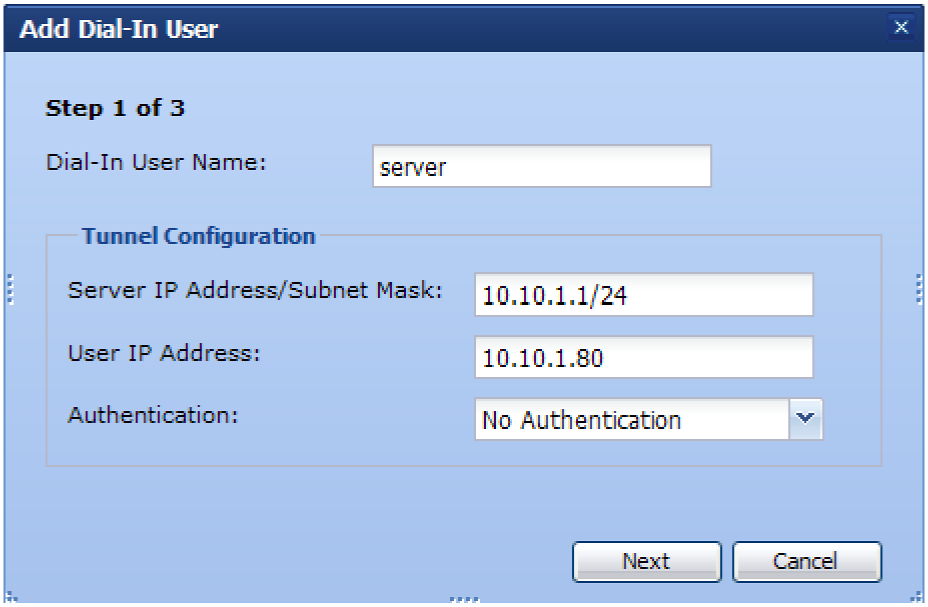
Parameter	**Setting for the Data Server Account**	**Setting for the Faculty Account**
Tunnel server IP address	10.*x*0.1.1/24	10.*x*1.1.1/24
Tunnel user IP address	10.*x*0.1.80	10.*x*1.1.85
Tunnel authentication	No Authentication	No Authentication
Policy group name	L2TPusers	L2TPusers
Authentication Protocol	MS-CHAP	MS-CHAP
User	server	faculty
Password	procurve1	procurve2
Default gateway	10.*x*0.1.1	10.*x*1.1.1
Primary DNS server	10.*x*0.10.10	10.*x*1.10.10

Note

The DNS value is used simply to illustrate how you would enter this value when configuring a user account. This lab does not require a DNS server for the clients.

Follow these steps to configure the dial-in user accounts.

1. On the ***VPN*** > ***IPsec*** > ***L2TP Remote Access*** window, click ***Add Dial-In User***.
2. For ***Dial-In User Name***, type ***server***.
3. For ***Server IP Address/Subnet Mask***, type ***10.x0.1.1/24***.
4. For ***User IP Address***, type ***10.x0.1.80***.
5. For ***Authentication***, select ***No Authentication***.



Add Dial-In User

Step 1 of 3

Dial-In User Name: server

Tunnel Configuration

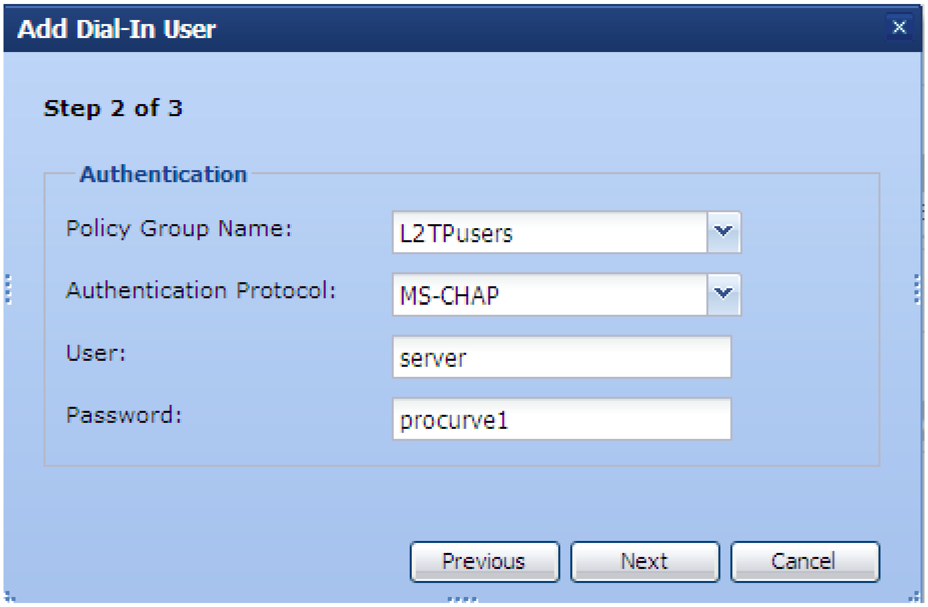
Server IP Address/Subnet Mask: 10.10.1.1/24

User IP Address: 10.10.1.80

Authentication: No Authentication

6. Click ***Next***.

7. For ***Policy Group Name***, select ***L2TPusers***.
8. For ***Authentication Protocol***, select ***MS-CHAP***.
9. For ***User***, type ***server***.
10. For ***Password***, type ***procurve1***.



Step 2 of 3

Authentication

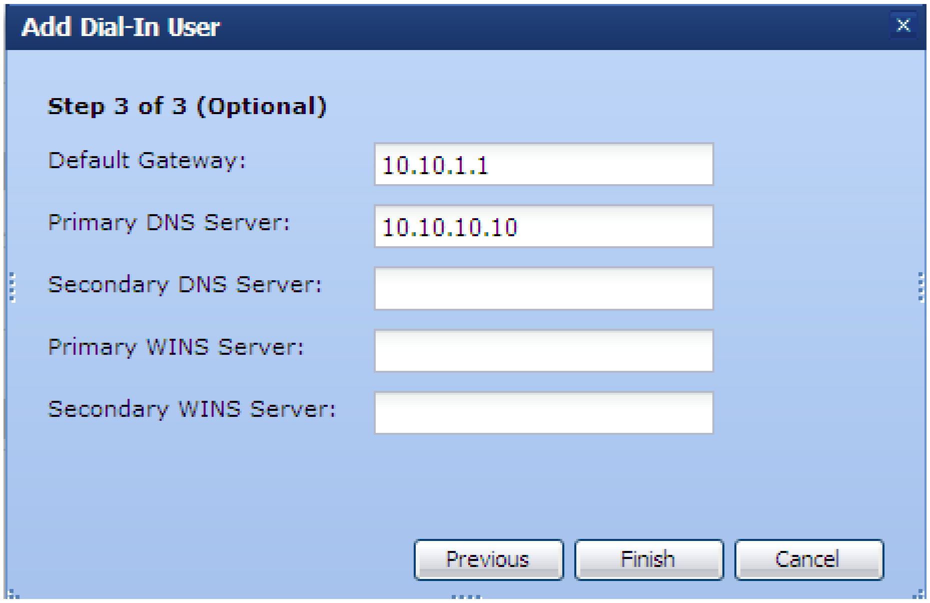
Policy Group Name: L2TPusers

Authentication Protocol: MS-CHAP

User: server

Password: procurve1

11. Click ***Next***.
12. For ***Default Gateway***, type ***10.x0.1.1***.
13. For ***Primary DNS Server***, type ***10.x0.10.10***.



Step 3 of 3 (Optional)

Default Gateway: 10.10.1.1

Primary DNS Server: 10.10.10.10

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

14. Click ***Finish***.
15. Click ***Save***.

16. Repeat the steps to create an account for the faculty member, using the settings shown in the table below.

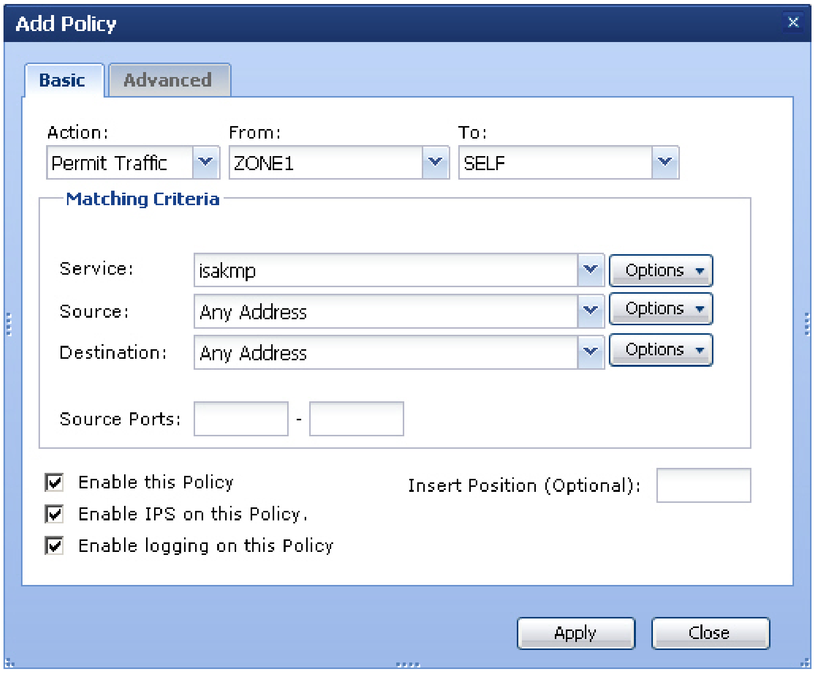
Parameter	**Setting for the Data Server Account**	**Setting for the Faculty Account**
Tunnel server IP address	10.*x*0.1.1/24	10.*x*1.1.1/24
Tunnel user IP address	10.*x*0.1.80	10.*x*1.1.85
Tunnel authentication	No Authentication	No Authentication
Policy group name	L2TPusers	L2TPusers
Authentication Protocol	MS-CHAP	MS-CHAP
User	server	faculty
Password	procurve1	procurve2
Default gateway	10.*x*0.1.1	10.*x*1.1.1
Primary DNS server	10.*x*0.10.10	10.*x*1.10.10

Task 7: Create Firewall Access Policies

You must configure firewall access policies that permit VPN clients to establish the tunnel. You must also configure policies that permit clients to send L2TP traffic to the TMS zl Module.

You will also set up an access policy that permits the faculty member to access the data server using the remote desktop program. Because only encrypted traffic is allowed, the access policy permits traffic between the *virtual* IP addresses used over the L2TP connection.

1. Click ***Firewall*** > ***Access Policies***.
2. Click the ***Unicast*** tab.
3. Click ***Add a policy*** and begin to create the access policies that permit devices in the data center to establish an L2TP over IPsec connection to the TMS zl Module.
4. For ***Action***, accept the default: ***Permit Traffic***.
5. For ***From***, select ***ZONE1***.
6. For ***To***, select ***SELF***.
7. For ***Service***, select ***isakmp***.
8. For ***Source*** and ***Destination*** accept the default settings: ***Any Address***.
9. Select the ***Enable logging on this Policy*** check box (leave the ***Enable this Policy*** and ***Enable IPS on this Policy*** check boxes selected).



Action: Permit Traffic

From: ZONE1

To: SELF

Matching Criteria

Service: isakmp

Source: Any Address

Destination: Any Address

Source Ports: -

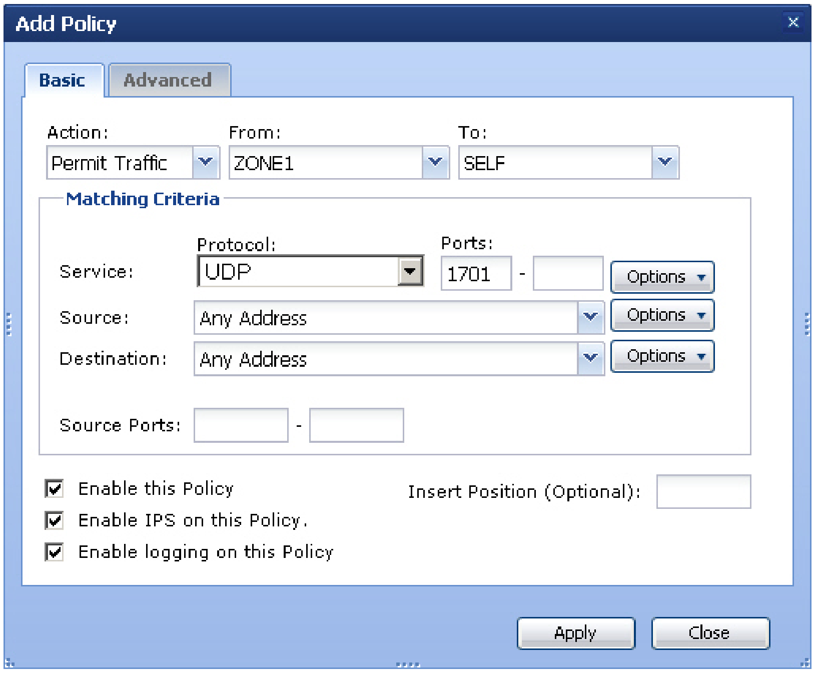
☑ Enable this Policy

☑ Enable IPS on this Policy.

☑ Enable logging on this Policy

Insert Position (Optional):

10. Click ***Apply***.
11. Configure the second access policy by accepting the default setting for ***Action***: ***Permit Traffic***.
12. Leave ***From*** and ***To*** at ***ZONE1*** and ***SELF***.
13. Enter a custom service.
    a. For ***Service***, click ***Options***.
    b. Click ***Enter custom Protocol/Port***.
    c. For ***Protocol***, select ***UDP***.
    d. For ***Ports***, type ***1701***.
14. For ***Source*** and ***Destination*** accept the defaults: ***Any Address***.
15. Leave the ***Enable this Policy***, ***Enable IPS on this Policy***, and ***Enable logging on this Policy*** check boxes selected.



Action: Permit Traffic
From: ZONE1
To: SELF
Matching Criteria
Service: Protocol: UDP Ports: 1701 -
Source: Any Address
Destination: Any Address
Source Ports: -
☑ Enable this Policy
☑ Enable IPS on this Policy.
☑ Enable logging on this Policy
Insert Position (Optional):

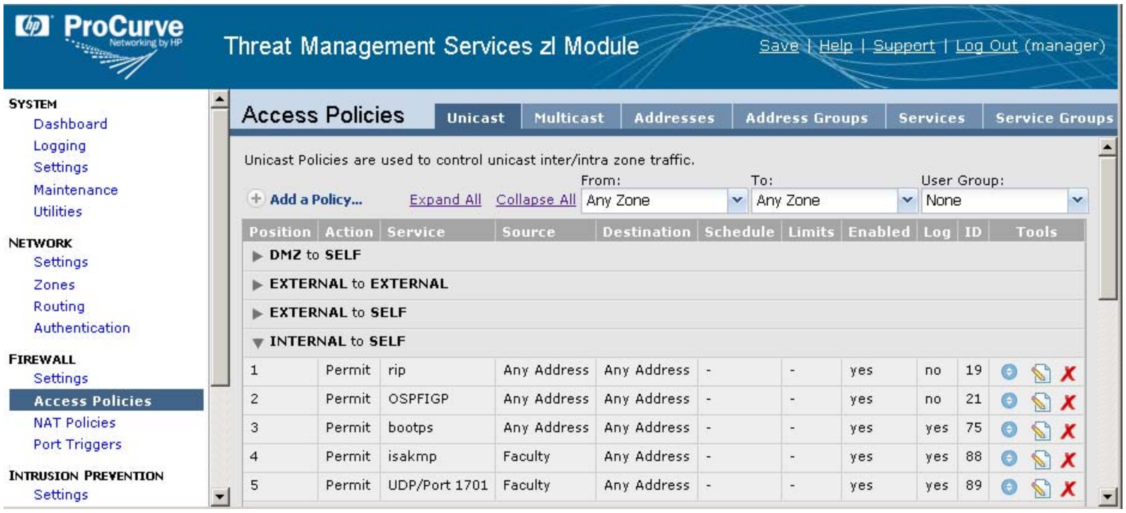
16. Click ***Apply***.

17. Repeat these steps to configure the rest of the access policies. Note that the zones for the access policy that controls traffic sent on the L2TP connection are both External.

Parameter	Access Policy 3	Access Policy 4	Access Policy 5
Action	Permit	Permit	Permit
From	INTERNAL	INTERNAL	EXTERNAL
To	SELF	SELF	EXTERNAL
Service	isakmp	Custom—UDP port 1701	RDP (using the service object that you created in *Lab 2: Configure the HP ProCurve TMS zl Module Firewall (Routing Mode)**
Source	Faculty address object	Faculty address object	10.*x*1.1.0/24
Destination	Any Address	Any Address	10.*x*0.1.0/24
Logging enabled	Yes	Yes	Yes

18. Click ***Close***.

When you have completed the configuration, you should see the Internal-to-Self access policies shown in the figure below.



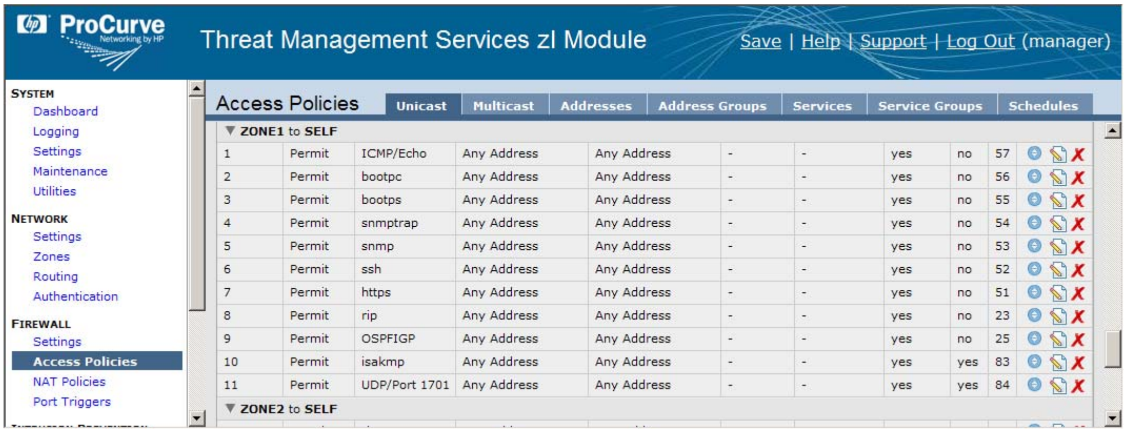
Access Policies

Unicast Policies are used to control unicast inter/intra zone traffic.

From: Any Zone   To: Any Zone   User Group: None

Position	Action	Service	Source	Destination	Schedule	Limits	Enabled	Log	ID	Tools
▶ DMZ to SELF										
▶ EXTERNAL to EXTERNAL										
▶ EXTERNAL to SELF										
▼ INTERNAL to SELF										
1	Permit	rip	Any Address	Any Address	-	-	yes	no	19	
2	Permit	OSPFIGP	Any Address	Any Address	-	-	yes	no	21	
3	Permit	bootps	Any Address	Any Address	-	-	yes	yes	75	
4	Permit	isakmp	Faculty	Any Address	-	-	yes	yes	88	
5	Permit	UDP/Port 1701	Faculty	Any Address	-	-	yes	yes	89	

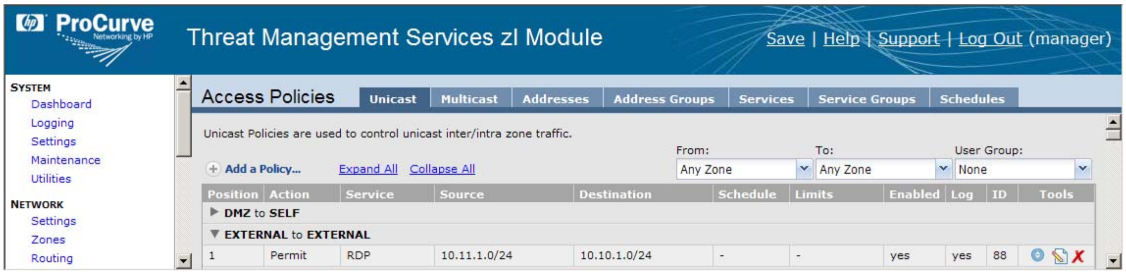
You should also see the Zone1-to-Self access policies shown in the figure below.



Access Policies

▼ ZONE1 to SELF									
1	Permit	ICMP/Echo	Any Address	Any Address	-	-	yes	no	57
2	Permit	bootpc	Any Address	Any Address	-	-	yes	no	56
3	Permit	bootps	Any Address	Any Address	-	-	yes	no	55
4	Permit	snmptrap	Any Address	Any Address	-	-	yes	no	54
5	Permit	snmp	Any Address	Any Address	-	-	yes	no	53
6	Permit	ssh	Any Address	Any Address	-	-	yes	no	52
7	Permit	https	Any Address	Any Address	-	-	yes	no	51
8	Permit	rip	Any Address	Any Address	-	-	yes	no	23
9	Permit	OSPFIGP	Any Address	Any Address	-	-	yes	no	25
10	Permit	isakmp	Any Address	Any Address	-	-	yes	yes	83
11	Permit	UDP/Port 1701	Any Address	Any Address	-	-	yes	yes	84
▼ ZONE2 to SELF									

You should also see the External-to-External access policy shown in the figure below.



Access Policies

Unicast Policies are used to control unicast inter/intra zone traffic.

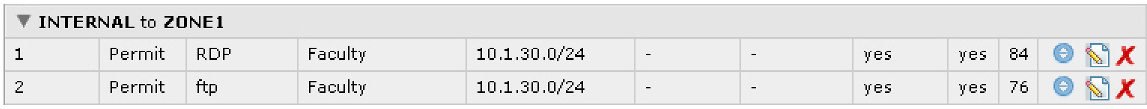
From: Any Zone   To: Any Zone   User Group: None

Position	Action	Service	Source	Destination	Schedule	Limits	Enabled	Log	ID	Tools
▶ DMZ to SELF										
▼ EXTERNAL to EXTERNAL										
1	Permit	RDP	10.11.1.0/24	10.10.1.0/24	-	-	yes	yes	88	

> **Note**
> Oftentimes when you configure VPN access for users who will establish a VPN across the Internet, their client is behind a NAT device. In such cases, you will need to configure access policies to permit the service ipsec-nat-t-udp (UDP/4500) between the Self zone and the appropriate access zone.

19. In Labs 2 and 3, you configured Internal-to-Zone1 policies that allowed faculty members to access the Windows Server 2003 over remote desktop and FTP. Remove those policies now so that the faculty members can only reach the data server after they have established the L2TP over IPsec connection.

    Locate the access policies and click the red X to delete them.



▼ INTERNAL to ZONE1

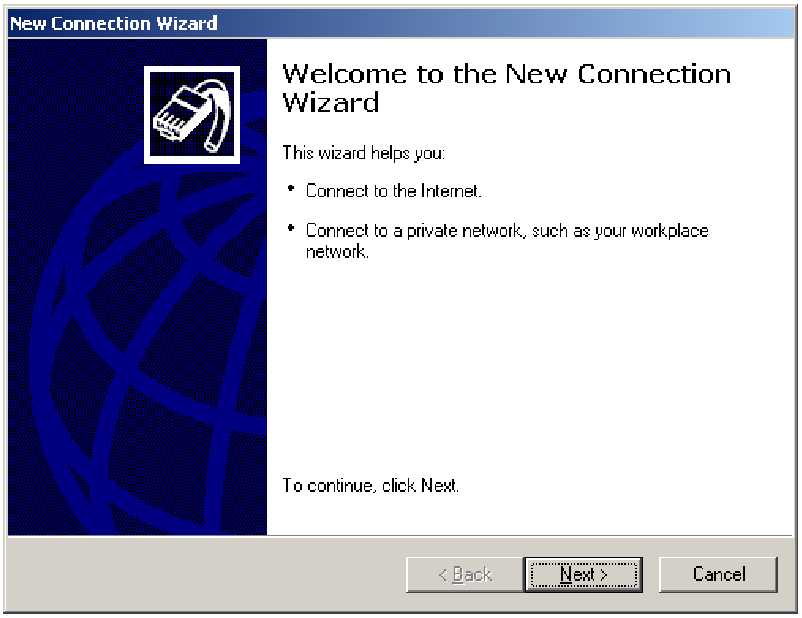
1	Permit	RDP	Faculty	10.1.30.0/24	-	-	yes	yes	84	⊖ ✎ ✗
2	Permit	ftp	Faculty	10.1.30.0/24	-	-	yes	yes	76	⊖ ✎ ✗

20. Click ***Save***.

Task 8: Configure the VPN Client on the Windows Server 2003 and on the Windows XP Pro Workstation

In this task, you will configure the L2TP over IPsec connection on both the Windows Server 2003 and the Windows XP workstation.

1. On the Windows Server 2003, click ***Start > Control Panel > Network Connections > New Connection Wizard***.



New Connection Wizard

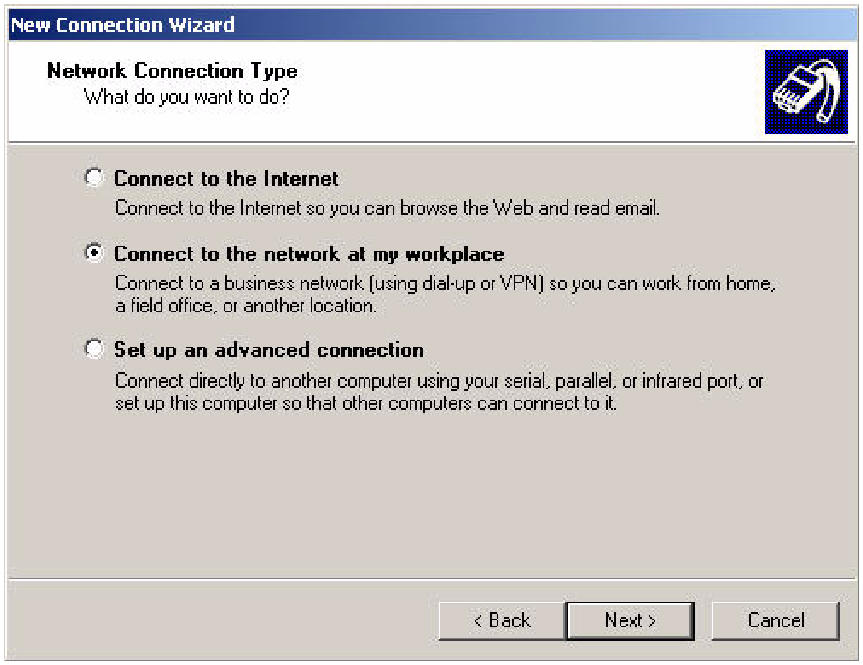
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.

To continue, click Next.

2. Click ***Next***.
3. Select ***Connect to the network at my workplace***.


New Connection Wizard

Network Connection Type
What do you want to do?

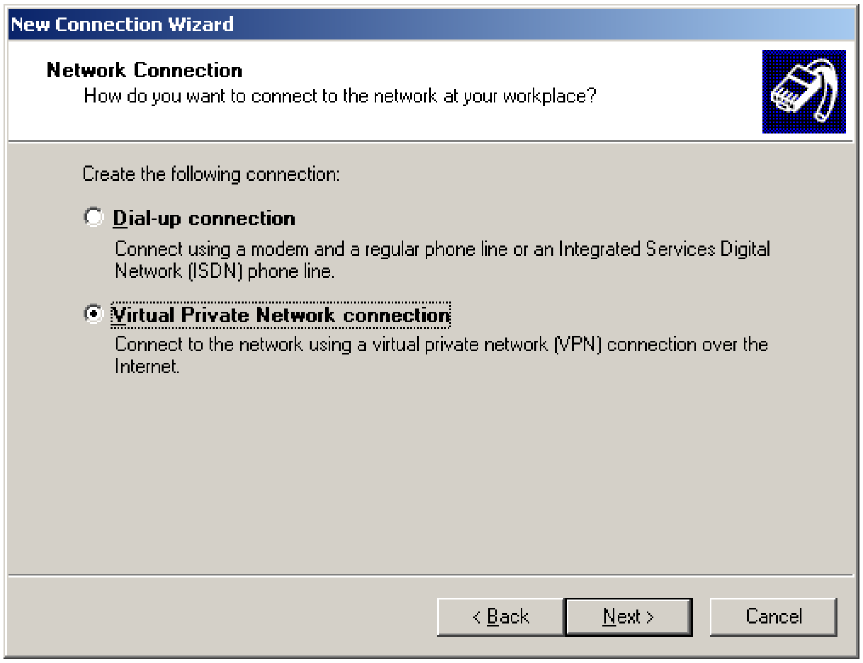
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

4. Click ***Next***.

5. Select ***Virtual Private Network connection***.


New Connection Wizard

Network Connection
How do you want to connect to the network at your workplace?

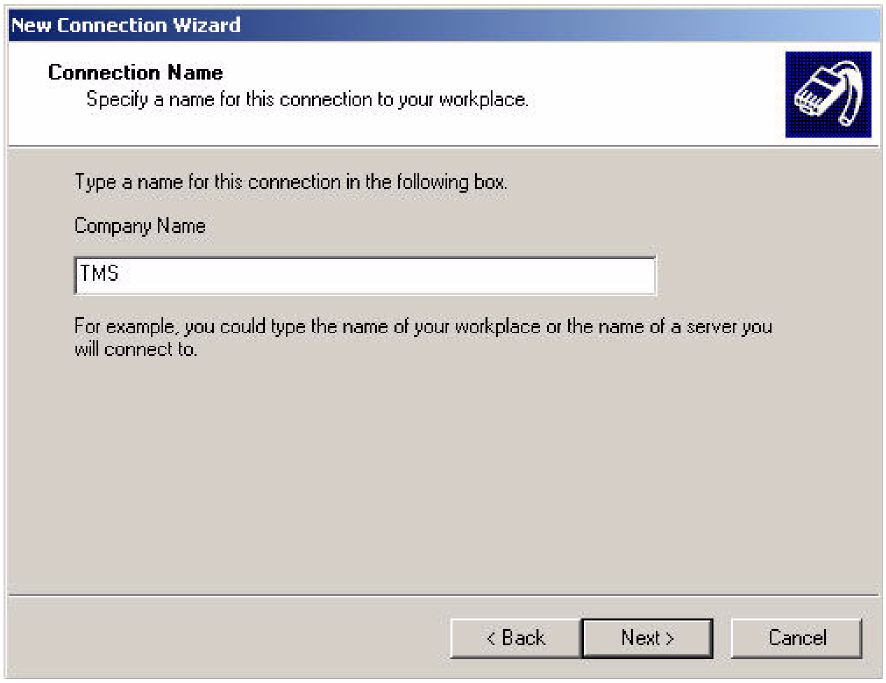
Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

6. Click ***Next***.

7. For ***Company Name***, type ***TMS***.



New Connection Wizard

Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

Company Name

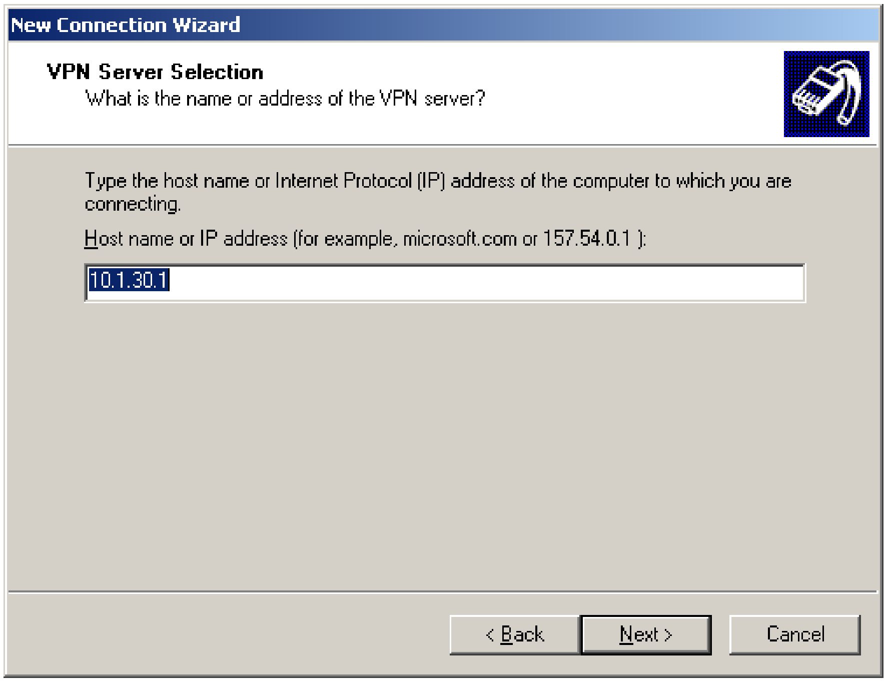
TMS

For example, you could type the name of your workplace or the name of a server you will connect to.

8. Click ***Next***.

9. If prompted, select ***Do not dial the initial connection*** and click ***Next***.

10. For ***Host name or IP address***, type ***10.x.30.1***.



New Connection Wizard

VPN Server Selection

What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

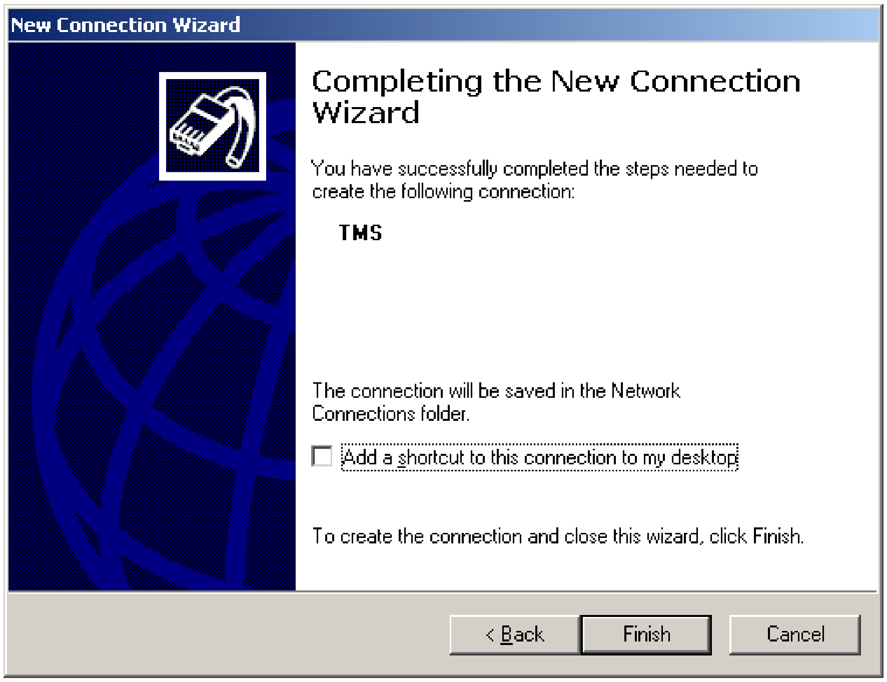
Host name or IP address (for example, microsoft.com or 157.54.0.1):

10.1.30.1

11. Click ***Next***.

12. If you are prompted if you want to use a smart card or a secured password, select secured password.

13. If prompted whether or not the connection can be shared, keep the default setting, ***My use only***, and click ***Next***.



New Connection Wizard

Completing the New Connection Wizard

You have successfully completed the steps needed to create the following connection:

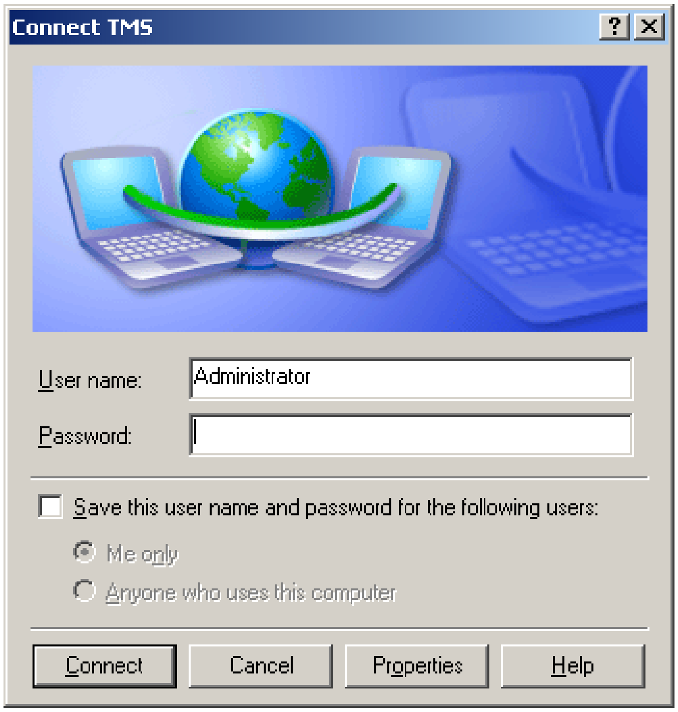
TMS

The connection will be saved in the Network Connections folder.

☐ Add a shortcut to this connection to my desktop

To create the connection and close this wizard, click Finish.

14. Select the ***Add a shortcut to this connection to my desktop***, and click ***Finish***. The ***Connect TMS*** window opens automatically.



Connect TMS

User name: Administrator

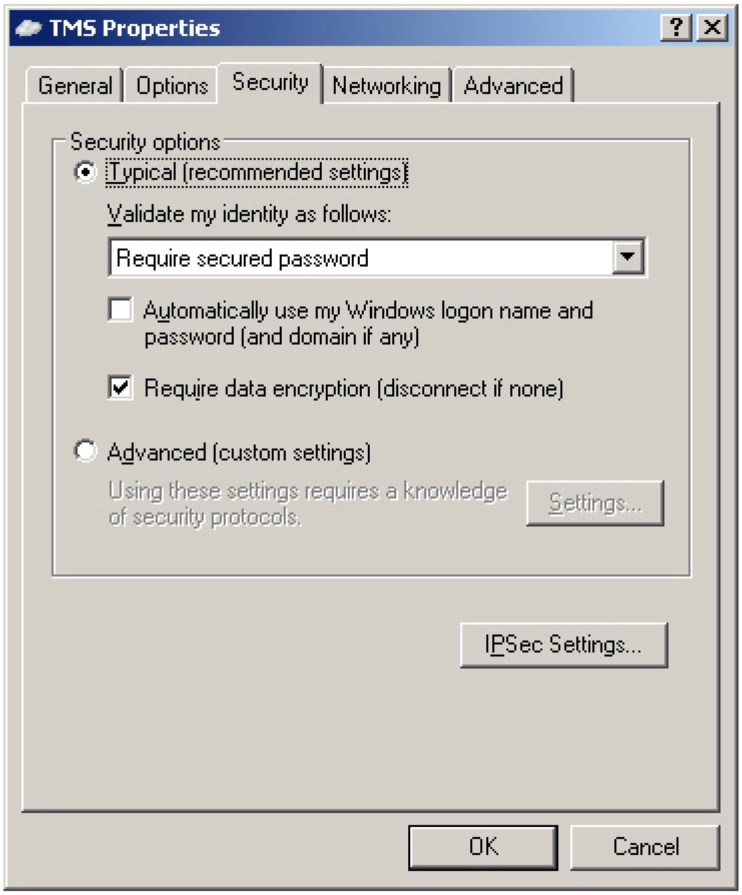
Password:

☐ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

15. Click ***Properties*** to open the connection properties window.
16. Click the ***Security*** tab.



Security options

● Typical (recommended settings)

Validate my identity as follows:

Require secured password

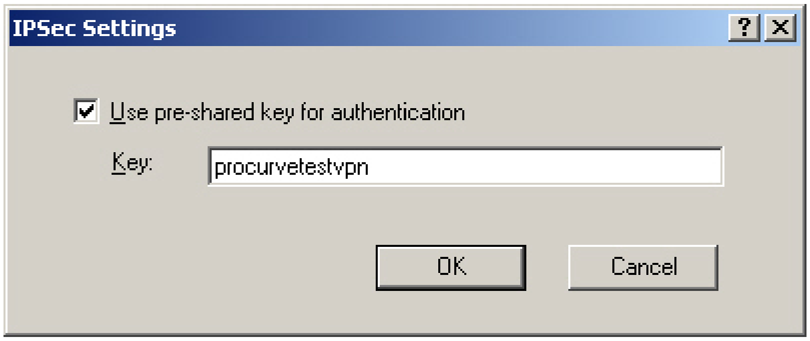
□ Automatically use my Windows logon name and password (and domain if any)

☑ Require data encryption (disconnect if none)

○ Advanced (custom settings)

Using these settings requires a knowledge of security protocols.

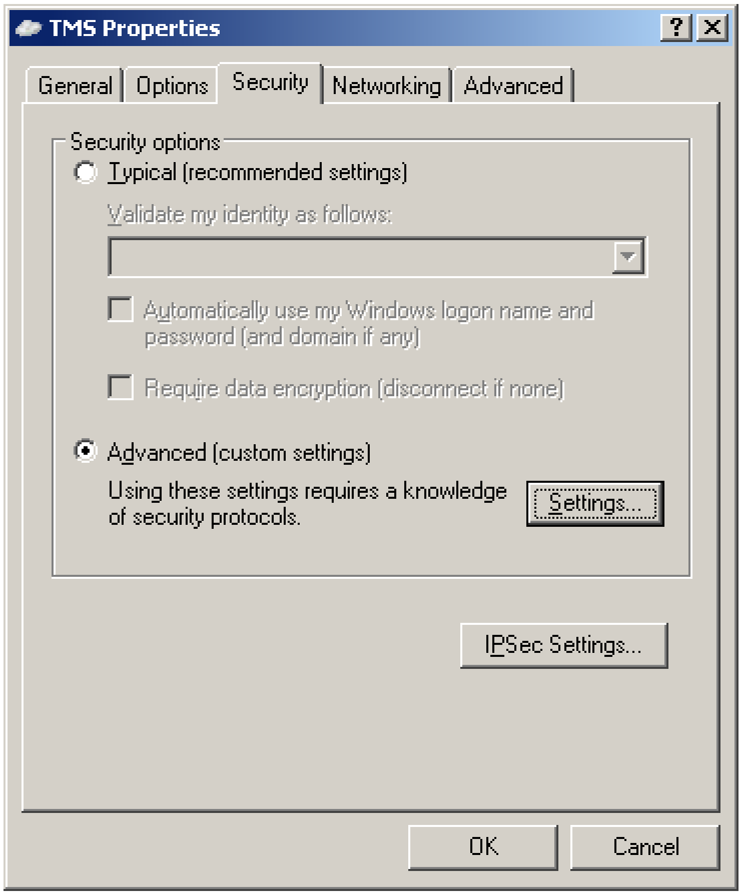
17. Click the ***IPsec Settings*** button.
18. Select ***Use pre-shared key for authentication***.



☑ Use pre-shared key for authentication

Key: procurvetestvpn

19. For ***Key***, type ***procurvetestvpn***.
20. Click ***OK***.



Security options

○ Typical (recommended settings)

Validate my identity as follows:

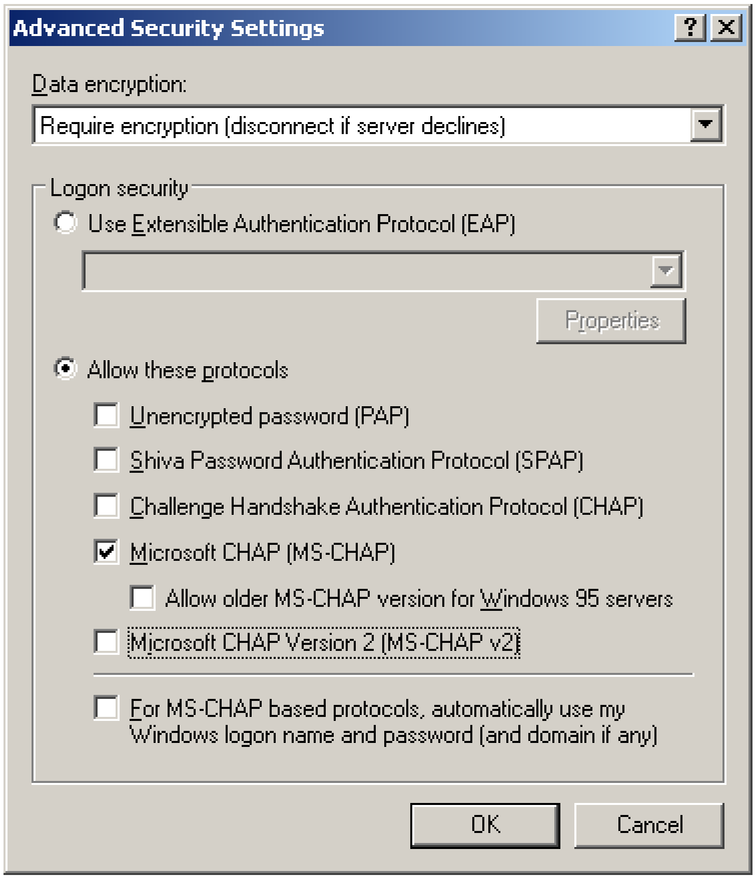
□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols. Settings...

21. Select ***Advanced (custom settings)*** and click ***Settings***.



Advanced Security Settings

Data encryption: Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

22. Select ***Allow these protocols***.
23. Clear all of the check boxes except for ***Microsoft CHAP (MS-CHAP)***.
24. Click **OK** to close each window until you return to the ***Connect TMS*** window.
25. Follow the same steps to configure the client on the Windows XP workstation.

Note

Ensure that the workstation is connected to port a4 and that it has received an IP address in VLAN 20.

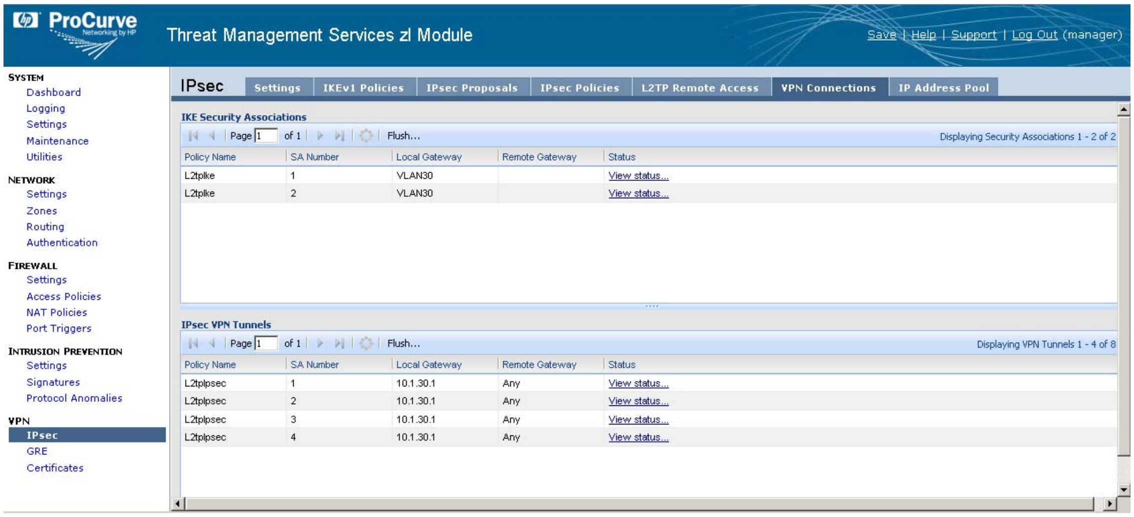
Also ensure that the IPsec service is running on the workstation, which you can determine by accessing the Control Panel and selecting ***Administrative Tools*** > ***Services***. If necessary, start the IPsec service.

A third-party VPN client can prevent you from starting the Windows IPsec service. Make sure that your Windows XP workstation does not have any such software installed (including HP ProCurve VPN Client).

Task 9: Establish the VPN

In this task, you first establish an L2TP over IPsec connection between the Windows Server 2003 and the TMS zl Module. You will keep that connection open so that authorized remote users can access the server. Next, you will log in to the L2TP over IPsec VPN as a faculty user on the Windows XP workstation. You will then test the connection by attempting to access the data server through remote desktop.

1. On the Windows Server 2003, double-click the TMS connection shortcut on the desktop.
2. Enter the L2TP user credentials:
   a. For ***User name***, type ***server***.
   b. For ***Password***, type ***procurve1***.
3. Click ***Connect***.
4. After a minute or so, you should see a message stating that the connection has been established.
5. Follow the same steps to establish the L2TP over IPsec connection on the Windows XP workstation. However, for ***User name***, type ***faculty*** and, for ***Password***, type ***procurve2***.
6. Check the connections in the TMS zl Web browser interface. Select ***VPN*** > ***IPsec***.
7. Click the ***VPN Connections*** tab.



IKE Security Associations

Displaying Security Associations 1 - 2 of 2

Policy Name	SA Number	Local Gateway	Remote Gateway	Status
L2tplke	1	VLAN30		View status...
L2tplke	2	VLAN30		View status...

IPsec VPN Tunnels

Displaying VPN Tunnels 1 - 4 of 8

Policy Name	SA Number	Local Gateway	Remote Gateway	Status
L2tplpsec	1	10.1.30.1	Any	View status...
L2tplpsec	2	10.1.30.1	Any	View status...
L2tplpsec	3	10.1.30.1	Any	View status...
L2tplpsec	4	10.1.30.1	Any	View status...

You should see four tunnels in the ***IPsec VPN Tunnels*** section:

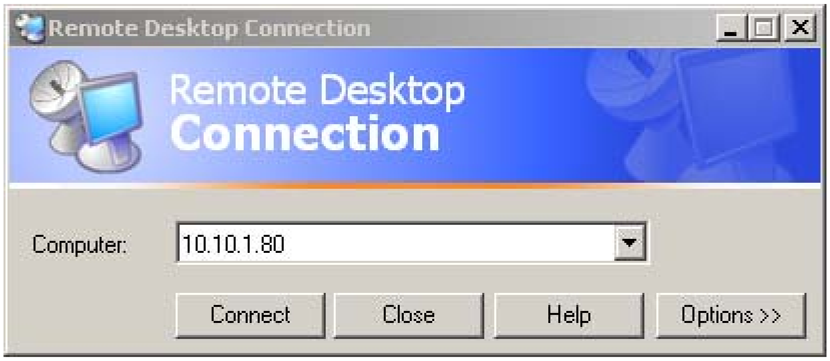
- An inbound tunnel for the connection between the Windows Server 2003 and the TMS zl Module
- An outbound tunnel for the connection between the server and the module
- An inbound tunnel for the connection between the Windows XP workstation and the module
- An outbound tunnel for the connection between the workstation and the module

You can view more information about each tunnel by clicking the ***View status*** link.

8. After you have verified that the connections have been established, attempt to access the data sever using the remote desktop program on the Windows XP workstation:

   a. Click ***Start*** > ***Programs*** > ***Accessories*** > ***Communications*** > ***Remote Desktop Connection***.

   b. Type the server's virtual L2TP address: ***10.x0.1.80***.



Computer: 10.10.1.80

   c. Click ***Connect***. You should be prompted to log in to the Windows Server 2003.

You have successfully completed this lab.