

## **Tru64 UNIX Best Practice**

---

### **Implementing IPsec Connections with Windows 2000 Peers**

**October 2002**

**Product Version: Tru64 UNIX**

**Operating System and Version: Version 5.1B**

This Best Practice describes how to set up a Tru64 UNIX system and a Windows 2000 system using IPsec to protect IP traffic between them.



---

# Contents

## Implementing IPsec Connections with Windows 2000 Peers

Is This Best Practice Right for You? .....	1
Before You Begin .....	1
A Sample Interoperability Scenario .....	2
Applying the Best Practice .....	3
Configuring Transport Mode IPsec Protection with IKE	
Preshared Key Authentication .....	3
Configuring the Tru64 UNIX System .....	4
Configuring the Windows 2000 System .....	5
Configuring Transport Mode IPsec Protection with IKE	
Public Key Certificate Authentication .....	8
Creating and Using the Public Key Certificates .....	8
Configuring the Tru64 UNIX System .....	14
Configuring the Windows 2000 System .....	15
Verifying Success .....	18
Troubleshooting .....	19
Alternative Practices .....	19
Comments and Questions .....	19
Legal Notice .....	19



---

# Implementing IPsec Connections with Windows 2000 Peers

This Best Practice describes how to set up a Tru64 UNIX system and a Windows 2000 system using IPsec to protect IP traffic between them.

See the Tru64 UNIX Best Practices Web page for more information about Best Practices documentation:

[http://www.tru64unix.compaq.com/docs/best\\_practices/](http://www.tru64unix.compaq.com/docs/best_practices/)

## Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that this Best Practice is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 5.1B
System Configuration	CDSA and IPsec
Need	To secure all IP traffic between a Tru64 UNIX system and a Windows 2000 system
Impact on Availability	None
Skills	Knowledge of IPsec and Windows 2000 environments

If you do not meet the previous requirements, see *Alternative Practices* for information.

## Before You Begin

Before you apply the Best Practice for implementing IPsec connections with Windows 2000 peers, you must understand some background information and perform some preliminary tasks.

- Understand Tru64 UNIX IPsec operation

You must know how to configure IPsec on a Tru64 UNIX system. See the *Network Administration: Connections* manual for more information.

- Understand Windows 2000 operation

You must have a thorough knowledge of Windows 2000 system administration; specifically, using the MMC Console. See the Windows 2000 documentation.

You should also know how IPsec operates on a Windows 2000 system. See the *Step-by-Step Guide to Internet Protocol Security (IPSec)* at the Microsoft Windows 2000 web site.

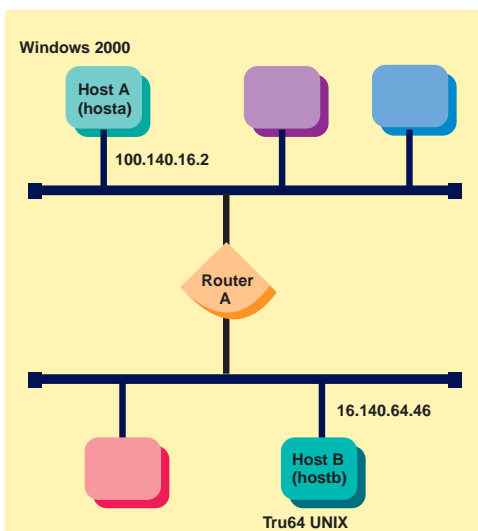
- Understand the Windows 2000 system's role

Is the system an Active Directory server? Is it supplying user authentication or host name resolution to the Tru64 UNIX system?

- Understand the interoperability scenario.

## A Sample Interoperability Scenario

The following illustration shows two separate local area networks (LANs) connected by a router that does not understand IPsec. In other words, the router only forwards packets from one LAN to the other.



ZK-1964U-AI

The following table lists information for each system in this scenario. You will use this information as you configure IPsec on each system.

	<b>hosta</b>	<b>hostb</b>
System type	Windows 2000 Server	Tru64 UNIX
IPv4 Address	100.140.16.2	16.140.64.46
IPsec protocol	ESP transport mode	ESP transport mode
Authentication method	3DES	3DES
Hash algorithm	MD5	MD5

Both systems will use the Encapsulating Security Payload (ESP) security protocol, which enables a receiver to verify both the identity of the sender and that the data has not been altered. It also provides confidentiality of the data through the use of encryption. Because the scenario involves creating a secure connection between two hosts, both systems will employ the ESP transport mode. In transport mode, the packet's IP header is the IP header for the resulting encrypted packet (payload and ESP trailer). For information about IPsec protocols and modes, see the *Network Administration: Connections* manual.

## Applying the Best Practice

Before you set up IPsec connections with Windows 2000 peers, be sure to follow the recommendations in *Before You Begin*. This section describes the following scenarios:

- Transport mode IPsec protection with IKE preshared key authentication
- Transport mode IPsec protection with IKE public key certificate authentication

## Configuring Transport Mode IPsec Protection with IKE Preshared Key Authentication

This section describes how to configure a Tru64 UNIX system and a Windows 2000 system to secure IP communications by using transport mode IPsec and authenticate the Internet Key Exchange (IKE) with preshared keys.

## Configuring the Tru64 UNIX System

For this scenario, run the SysMan IPsec application on the Tru64 UNIX system and do the following:

1. If you are using static routes, go to step 2. If you are using `gated` or `routed` to obtain routing information, add an `allow-rip` connection with the following information. This enables Routing Internet Protocol (RIP) traffic to be sent and received without IPsec protection.
  - Remote IP Address Selector: All IPv4 addresses, UDP protocol, and port 520.
  - Local IP Address Selector: All IPv4 addresses, UDP protocol, and port 520.
  - Action: Pass without IPsec protection.
2. If single sign-on (SSO) is not enabled on your system, go to step 4. If SSO is enabled on your system, `hosta` is supplying you with user authentication services. Create an `allow-krb5-io` connection with the following information:
  - Remote IP Address Selector: All IPv4 addresses, UDP protocol, and port 88.
  - Local IP Address Selector: All IPv4 addresses, UDP protocol, and port 88.
  - Action: Pass without IPsec protection.
3. Add a `hostb-hosta` connection with the following information. This enables IP traffic to and from `hosta` to be sent and received with IPsec protection.
  - Remote IP Address Selector: Single IPv4 address 100.140.16.2
  - Local IP Address Selector: Single IPv4 address 16.140.64.46
  - Action: Apply IPsec protection
  - IPsec Proposal List: `ESP-transport-proposals`
  - Obtain Keys: Via Internet Key Exchange (IKE) Protocol
  - IKE Proposal List: `+Pre-Shared-Key-Proposals`, consisting of 3DES encryption and either SHA1 or MD5 hashing
  - Authenticate IKE exchanges: via pre-shared IKE key
  - Key Name: `hostb-hosta-secret`
  - Key Value: `secret-between-hosta-and-hostb`

- Local Identity: IPv4 Address: 16.140.64.46
4. If `hosta` is a Windows 2000 Active Directory server and it is providing host name resolution to the Tru64 UNIX system, select the `allow-dns-io` connection and move it below the `hostb-hosta` connection. If you do not, your system will be unable to resolve host names.

## Configuring the Windows 2000 System

For this scenario, do the following on the Windows 2000 system:

1. Add an IP Security Policy Management snap-in. If the snap-in has already been added, go to step 2.
  - a. From the Windows desktop, click Start, click Run, and in the Open text box enter `mmc`.
  - b. In the console window, enter `ctrl-m` to display the Add/Remove Snap-in dialog box.
  - c. Click Add to display the Add Standalone Snap-in dialog box.
  - d. Select IP Security Policy Management, then click Add.
  - e. In the Select Computer dialog box, click Local Computer, then click Finish.
  - f. Close the Add Standalone Snap-in dialog box, then select OK in the Add/Remove Snap-in dialog box.

An IP Security Policies on Local Machine entry now appears under the Console Root in the left pane.

2. Add a security policy group. Do the following:
  - a. Select IP Security Policies on Local Machine in the left pane of the MMC console. The right pane of the console displays default policy entries similar to the following:
 

```
Client (Respond only)
Secure server (Require Security)
Server (Request Security)
```
  - b. Right click the IP Security Policies on Local Machine entry in the left pane. Then, left click to select Create IP Security Policy. The IP Security Policy Wizard is displayed. Select Next.
  - c. Enter a policy name. For this scenario, enter `My test policy 1`. Then, click Next.

- d. Deactivate the `Activate the default response rule` check box in the `Requests for Secure Communication` dialog box.
    - e. Select the `Edit Properties` check box in the next dialog box.
    - f. Select `Finish`. The `My test policy 1` entry is displayed in the right pane.
  3. Add a filter list to filter traffic from `100.140.16.2` to `16.140.64.46`. Do the following:
    - a. Double click the `My test policy 1` entry in the right pane.
    - b. Clear the `Use Add Wizard` check box in the `My test policy 1 Properties` dialog box.
    - c. Select `Add` in the `My test policy 1 Rules` tab. The `New Rule Properties` dialog box is displayed.
    - d. Select `Add` in the `IP Filter List` tab. The `IP Filter List` dialog box is displayed.
    - e. Type the filter name. For this scenario, enter `hosta-hostb`.
    - f. Clear the `Use Add Wizard` check box.
    - g. Select `Add` in the `IP Filter List` dialog box.
    - h. Select `A specific IP Address`, then enter a source address (`100.140.16.2`) in the `Addressing` tab of the `Filter Properties` dialog box.
    - i. Select `A specific IP Address`, then enter a destination address (`16.140.64.46`) in the `Addressing` tab of the `Filter Properties` dialog box.
    - j. Check the `Mirrored` check box.
    - k. Select the `protocol` tab of the `Filter Properties` dialog box and select `Any` as the protocol type. Then select `OK` in the `Filter Properties` dialog box.
    - l. Close the `IP Filter List` dialog box.
  4. Add a rule for the `hosta-hostb` filter. Do the following:
    - a. Click the `hosta-hostb` entry in the `IP Filter List` tab.
    - b. Click the `Tunnel Setting` tab and select `This rule does not specify an IPSec tunnel`.
    - c. Select the `Connection Type` tab and select `Local Area Network (LAN)`.

- d. Click the Filter Action tab and clear the Use Add Wizard check box.
  - e. Select Add in the Filter Action tab.
  - f. Select Negotiate Security in the New Filter Action Properties dialog box. Clear the Accept unsecured communication, but always respond using IPsec check box.
  - g. Select Add in the New Filter Action Properties dialog box. Then, select Custom (for expert users). Click Settings to display the Custom Security Settings dialog box.
  - h. Select Data integrity and encryption (ESP) and select 3DES as the encryption algorithm because hostb is configured to use ESP and 3DES authentication. Then, click OK to display the New Security Method dialog box. Then, select OK to display the New Filter Action Properties dialog box.
  - i. Select the General tab and specify the filter action you just created (for this scenario, enter `my high security (ESP)`).
  - j. Click OK to return to the Filter Action tab.
  - k. Click the `my high security (ESP)` radio button to choose the newly created filter action for the `hosta-hostb` filter.
  - l. Select Authentication Methods tab and select Edit to change the authentication method.
  - m. Select Use this string to protect the key exchange (preshared key) and enter the string (for this scenario, enter `secret-between-hosta-and-hostb`).
  - n. Click OK to return to the Authentication Methods tab.
  - o. Click OK to return to the My test policy 1 Properties dialog box. The `hosta-hostb` rule is displayed.
  - p. Close the My test policy 1 Properties dialog box.
5. Assign the new policy to the Windows 2000 server. Do the following:
- a. Right click `My test policy 1` entry on the right pane of the MMC console and select Assign. The Policy Assigned column of the `My test policy 1` entry should indicate yes.
  - b. Close the MMC console.

## Configuring Transport Mode IPsec Protection with IKE Public Key Certificate Authentication

This section describes how to configure a Tru64 UNIX system and a Windows 2000 system to secure IP communications by using transport mode IPsec and authenticate the Internet Key Exchange (IKE) with public key certificates. This section describes the following:

- Creating and using public key certificates
- Configuring the Tru64 UNIX system
- Configuring the Windows 2000 system

### Creating and Using the Public Key Certificates

Creating and using the public key certificates consists of the following steps:

1. On the Tru64 UNIX system, creating a storage directory and certificates.
2. On the Windows 2000 system, doing the following:
  - a. Installing required software components
  - b. Copying and importing the CA certificate from the Tru64 UNIX system
  - c. Creating a certificate for the Windows 2000 system
  - d. Exporting the Windows 2000 certificate
3. On the Tru64 UNIX system, copying the public key certificate from the Windows 2000 system and adding it to the IPsec configuration.

#### Tru64 UNIX Certificate Tasks - 1

On the Tru64 UNIX system, do the following:

1. Change to the `/var/ipsec` directory.
2. Create a CA certificate and private key. Do the following:
  - a. If you already have a signed CA certificate, copy the certificate and private key file to the `/var/ipsec` directory and write down the file names and their format (for example, binary, PEM, or HEXL). You will need this information when you configure IPsec (run the SysMan IPsec application) on the Tru64 UNIX system. Go to step 3.

- b. Create a file called `mycorp-rsa-ca.x509` with the following information:

```
Certificate ::= {
  Outputfile ::= "mycorp-rsa-ca.cer"

  SerialNumber ::= 0
  SubjectName ::= <C=US,O=Mycorp\, Inc., CN=IPsec Test CA>
  IssuerName ::= <C=US,O=Mycorp\, Inc., CN=IPsec Test CA>
  Validity ::= {
    NotBefore ::= "1998/06/30/19:30:00"
    NotAfter ::= "2004/01/01/12:30:00"
  }
  PublicKeyInfo ::= {
    Size ::= 1024
    Type ::= rsaEncryption
    PrivateKeyFile ::= "mycorp-rsa-ca.prv"
  }
  Signature ::= {
    SelfSigned
    SignatureAlgorithm ::= shaWithRSAEncryption
  }
  Extensions ::= {
    SubjectAltNames ::= {
      IP ::= 16.140.64.46
      EMAIL ::= jones@site.mycorp.com
    }
    ExtendedKeyUsage ::= {
      ServerAuth
      ClientAuth
      CodeSigning
      EmailProtection
      TimeStamping
      IkeIntermediate
    }
    BasicConstraints ::= {
      CA
      PathLength ::= 0
    }
    KeyUsage ::= {
      DigitalSignature
      KeyCertSign
    }
  }
}
```

- c. Create the CA certificate with the following command:

```
# /usr/sbin/ipsec_certmake mycorp-rsa-ca.x509
```

The `mycorp-rsa-ca.cer` certificate file and `mycorp-rsa-ca.prv` private key file are created in the current directory.

3. Create a public key certificate and private key for hostb. Do the following:
  - a. If you already have a public key certificate for hostb, copy the certificate and private key file to the /var/ipsec directory and write down the file names and their format (for example, binary, PEM, or HEXL). You will need this information when you configure you run the SysMan IPsec application. Go to the Windows 2000 Certificate Tasks section at the end of this section.
  - b. Create a file called mycorp-rsa-hostb.x509 with the following information:

```

Certificate ::= {
  Outputfile ::= "mycorp-rsa-hostb.cer"

  SerialNumber ::= 1
  SubjectName ::= <C=US,O=Mycorp\, Inc., CN=HOSTB>
  IssuerName ::= <C=US,O=Mycorp\, Inc., CN=IPsec Test CA>
  Validity ::= {
    NotBefore ::= "1999 Jul 30th, 19:30:00"
    NotAfter ::= "2003 Dec 1st, 12:30:00"
  }
  PublicKeyInfo ::= {
    Size ::= 1024
    Type ::= rsaEncryption
    PrivateKeyFile ::= "mycorp-rsa-hostb.prv"
  }
  Signature ::= {
    SignatureAlgorithm ::= shaWithRSAEncryption
    IssuerKeyFile ::= "mycorp-rsa-ca.prv"
  }
  Extensions ::= {
    SubjectAltNames ::= {
      IP ::= 16.140.64.46
    }
    KeyUsage ::= {
      DigitalSignature
      KeyEncipherment
    }
  }
}

```

- c. Create the certificate for hostb with the following command:

```
# /usr/sbin/ipsec_certmake mycorp-rsa-hostb.x509
```

The mycorp-rsa-hostb.cer certificate file and mycorp-rsa-hostb.prv private key file are created in the current directory.

## Windows 2000 Certificate Tasks

On the Windows 2000 system, complete the following steps:

1. Install the High Encryption Pack for Windows 2000 or Windows 2000 Service Pack 2, if it is not already installed. You can obtain the pack from the following location:

[www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp](http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp)

After installing the pack, reboot your system.

2. If your system is already in a Windows 2000 Active Directory domain, go to step 3. Otherwise, install the Active Directory service. Do the following:
  - a. Select Active Directory from the Configure Your Server Wizard.
  - b. Click the Start the Active Directory wizard link and select the following options:
    - Domain controller for a new domain.
    - Create a new domain tree.
    - Create a new forest of domain trees.
    - Full DNS name for the new domain. For this scenario, enter `ipsec.mycorp.com`.
    - Domain: NETBIOS (the default).
    - Install and configure DNS on the system.
  - c. Reboot your system.
3. If Certificate Services is already installed, write down the CA name and go to step 4. Otherwise, install Certificate Services. Do the following:
  - a. Click Start, click Settings, click Control Panel, click Add-Remove Programs, then click Add-Remove Windows Components tab.
  - b. Select Configure under the Certificate Services entry.
  - c. Modify the Enterprise root CA settings and the advanced options as follows:
    - CSP = Microsoft Enhanced Cryptographic Provider V1.0
    - Hash algorithm = SHA-1

- Key length = 1024
- d. Enter a CA name (for this scenario, enter `mycorp_ipsec_ca2`), Organization (O), Organizational Unit (OU), city, state, country, Email address, CA description, Validity, and so on.
4. If the Certification Authority snap-in is already installed, go to step 5. Otherwise, add a Certification Authority (local) snap-in. Do the following:
    - a. Enter `mmc` at the command prompt.
    - b. In the console1 window, enter `ctrl-m` to display the Add/Remove Snap-in dialog box.
    - c. Click Add to display the Add Standalone Snap-in dialog box.
    - d. Select Certification Authority and click Add.
    - e. In the Certification Authority dialog box, select Local Computer, then click Finish.
    - f. Close the Add Standalone Snap-in dialog box, then click OK in the Add/Remove Snap-in dialog box.

A Certification Authority entry now appears under the Console Root in the left pane.
  5. If the Certificates snap-in is already installed, go to step 6. Otherwise, add a Certificates (computer account, local computer) snap-in. Do the following:
    - a. Enter `mmc` at the command prompt.
    - b. In the console1 window, enter `ctrl-m` to display the Add/Remove Snap-in dialog box.
    - c. Click Add to display the Add Standalone Snap-in dialog box.
    - d. Select Certificates and click Add.
    - e. In the Certificates Snap-in dialog box, select Computer Account, then click Next.
    - f. In the Select Computer dialog box, select Local Computer, then click Finish.
    - g. Close the Add Standalone Snap-in dialog box, then click OK in the Add/Remove Snap-in dialog box.

A Certificates entry now appears under the Console Root in the left pane.

6. Copy the Mycorp CA certificate file (`mycorp-rsa-ca.cer`) from Host B to any temporary directory on Host A.
7. Import the Mycorp CA certificate. Click Certificates (local computer), click Trusted Root Certification Authorities, click Certificates, right click All Task, and click Import. Follow the Certificate Import Wizard to import the Mycorp CA certificate.
8. Create a certificate for `hosta`. Do the following:
  - a. Open Certificates from the MMC console.
  - b. Right click on the Personal/Certificates folder.
  - c. Select All Task/Request New Certificate.
  - d. Select the Advanced options and select Microsoft Enhanced Cryptographic Provider V1.0 from the list. Continue with the process. This creates a certificate for `hosta`.
9. Verify that the certificate was created by selecting Personal/Certificates. A certificate for `hosta.ipsec.mycorp.com` by CA `mycorp_ipsec_ca2` (or the CA already set up on the system) for the purpose of client authentication is displayed. In addition, the self-signed CA certificate by CA `mycorp_ipsec_ca2` (or the CA already set up on the system) is displayed. Double click on a certificate to see more detail.
10. Export `hosta`'s CA certificate. Do the following:
  - a. Open Certificates (local computer).
  - b. Select Trusted Root Certification Authorities and click Certificates.
  - c. Right click on the Windows 2000 (`hosta`'s) CA, click All Task, and click Export.
  - d. In the export wizard, select DER encoded binary X.509 as the format and enter a file name (for this scenario, enter `w2k_mycorp_ipsec_ca2.cer`).

## Tru64 UNIX Certificate Tasks - 2

On the Tru64 UNIX system, complete the following steps:

1. Copy the `w2k_mycorp_ipsec_ca2.cer` file from `hosta` to the `/var/ipsec` directory on `hostb`.
2. Run the SysMan IPsec application.

3. Add a public key certificate for `hosta` with the following information:
  - Certificate Name: `w2k-mycorp-ipsec-ca2-cer`
  - Certificate Encoding: Binary
  - Certificate File: `/var/ipsec/w2k_mycorp_ipsec_ca2.cer`

### Configuring the Tru64 UNIX System

For this scenario, do the following on the Tru64 UNIX system:

1. Run the SysMan IPsec application.
2. If you are using static routes, go to step 3. If you are using `gated` or `routed` to obtain routing information, create an `allow-rip` connection with the following information. This enables Routing Internet Protocol (RIP) traffic to be sent and received without IPsec protection.
  - Remote IP Address Selector: All IPv4 addresses, UDP protocol, and port 520.
  - Local IP Address Selector: All IPv4 addresses, UDP protocol, and port 520.
  - Action: Pass without IPsec protection.
3. If single sign-on (SSO) is not enabled on your system, go to step 4. If SSO is enabled on your system, `hosta` is supplying you with user authentication services. Create an `allow-krb5-io` connection with the following information:
  - Remote IP Address Selector: All IPv4 addresses, UDP protocol, and port 88.
  - Local IP Address Selector: All IPv4 addresses, UDP protocol, and port 88.
  - Action: Pass without IPsec protection.
4. Create a `hostb-hosta` connection with the following information. This enables IP traffic to and from `hosta` to be sent and received with IPsec protection.
  - Remote IP Address Selector: Single IPv4 address 100.140.16.2
  - Local IP Address Selector: Single IPv4 address 16.140.64.46
  - Action: Apply IPsec protection
  - Proposal List: `+ESP-transport-proposals`
  - Obtain Keys: Via Internet Key Exchange (IKE) Protocol

- IKE Proposal List: `RSA-signature-proposals`, consisting of 3DES encryption and either SHA1 or MD5 hashing
  - Authenticate IKE exchanges: via public-key certificate
  - Certificate Name: `mycorp-rsa-hostb-cer`
  - Certificate Emcoding: Binary
  - Certificate File: `/var/ipsec/mycorp-rsa-hostb.cer`
  - Private Key Encoding: Binary
  - Private Key File: `/var/ipsec/mycorp-rsa-hostb.prv`
  - IKE Group: 2
5. If `hosta` is a Windows 2000 Active Directory server and it is providing host name resolution to the Tru64 UNIX system, select the `allow-dns-io` connection and move it below the `hostb-hosta` connection. If you do not, your system will be unable to resolve host names.
  6. Select Enable IP Security (IPsec) for this system.
  7. Select OK to save the changes and start IPsec.

### Configuring the Windows 2000 System

For this scenario, do the following on the Windows 2000 system:

1. Add an IP Security Policy Management snap-in. If the snap-in has already been added, go to step 2.
  - a. Enter `mmc` at the command prompt.
  - b. In the console1 window, enter `ctrl-m` to display the Add/Remove Snap-in dialog box.
  - c. Click Add to display the Add Standalone Snap-in dialog box.
  - d. Select IP Security Policy Management, then click Add.
  - e. In the Select Computer dialog box, select Local Computer, then click Finish.
  - f. Close the Add Standalone Snap-in dialog box, then click OK in the Add/Remove Snap-in dialog box.

An IP Security Policies on Local Machine entry now appears under the Console Root in the left pane.

2. Add a security policy group. Do the following:
  - a. Select IP Security Policies on Local machine in the left pane of the MMC console. The right pane of the console displays default policy entries similar to the following:

```
Client (Respond only)
Secure server (Require Security)
Server (Request Security)
```
  - b. Right click the IP Security Policies on Local machine entry in the left pane. Then, left click to select Create IP Security Policy. The IP Security Policy Wizard is displayed. Select Next.
  - c. Enter a policy name. For this scenario, enter `My test policy 1`. Then, click Next.
  - d. Deactivate the `Activate the default response rule` check box in the Requests for Secure Communication dialog box.
  - e. Select the `Edit properties` check box in the next dialog box.
  - f. Select Finish. The `My test policy 1` entry is displayed in the right pane.
3. Add a filter list to filter traffic from 100.140.16.2 to 16.140.64.46. Do the following:
  - a. Double click the `My test policy 1` entry in the right pane.
  - b. Clear the `Use Add Wizard` check box in the `My test policy 1 Properties` dialog box.
  - c. Select `Add` in the `My test policy 1 Rules` tab. The `New Rule Properties` dialog box is displayed.
  - d. Select `Add` in the `IP Filter List` tab. The `IP Filter List` dialog box is displayed.
  - e. Enter the filter name. For this scenario, enter `hosta-hostb`.
  - f. Clear the `Use Add Wizard` check box.
  - g. Click `Add` in the `IP Filter List` dialog box.
  - h. Select `A specific IP Address`, then enter a source address (100.140.16.2) in the `Addressing` tab of the `Filter Properties` dialog box.
  - i. Select `A specific IP Address`, then enter a destination address (16.140.64.46) in the `Addressing` tab of the `Filter Properties` dialog box.
  - j. Check the `Mirrored` check box.

- k. Select the Protocol tab of the Filter Properties dialog box and select Any as the protocol type. Then click OK in the Filter Properties dialog box.
  - l. Close the IP Filter List dialog box.
4. Add a rule for the `hosta-hostb` filter. Do the following:
- a. Double click the `hosta-hostb` entry in the IP Filter List tab.
  - b. Click the Tunnel Setting tab and select This rule does not specify an IPsec tunnel.
  - c. Select the Connection Type tab and select Local Area Network (LAN).
  - d. Click the Filter Action tab and clear the Use Add Wizard check box.
  - e. Select Add in the Filter Action tab.
  - f. Select Negotiate Security in the New Filter Action Properties dialog box. Clear the Accept unsecured communication, but always respond using IPsec check box.
  - g. Select Add in the New Filter Action Properties dialog box. Then, select Custom (for expert users). Click Settings to display the Custom Security Settings dialog box.
  - h. Select Data integrity and encryption (ESP) and select 3DES as the encryption algorithm because `hostb` is configured to use ESP and 3DES authentication. Then, click OK to display the New Security Method dialog box. Then, select OK to display the New Filter Action Properties dialog box.
  - i. Select the General tab and specify the filter action you just created (for this scenario, enter `my high security (ESP)`).
  - j. Click OK to return to the Filter Action tab.
  - k. Click the `my high security (ESP)` radio button to choose the newly created filter action for the `hosta-hostb` filter.
  - l. Select Authentication Methods tab and click Edit to change the authentication method.
  - m. Select Use a certificate from this Certificate Authority (CA) and click Browse.

- n. Select the CA certificate that you previously imported and click OK. Click OK again to return to the Authentication method preference order list.
  - o. Click Add. The New Authentication Method Properties dialog box is displayed.
  - p. Select Use a certificate from this Certificate Authority (CA) and select Browse.
  - q. Select the Windows 2000 CA (`mycorp_ipsec_ca2` or the name of the CA that is already installed) and click OK. Click OK again to return to the Authentication method preference order list. Two CAs are displayed. Authentication will validate any certificate issued by either of the two CAs.
  - r. Click OK to return to the `My test policy 1` Properties dialog box. The `hosta-hostb` rule is displayed.
  - s. Close the `My test policy 1` Properties dialog box.
5. Assign the new policy to the Windows 2000 server. Do the following:
    - a. Right click the `My test policy 1` entry on the right pane of the MMC console and select Assign. The Policy Assigned column of the `My test policy 1` entry should indicate `yes`.

## Verifying Success

After you apply this Best Practice for implementing IPsec connections with Windows 2000 peers, you can verify whether it was successful. From the Windows 2000 system (`hosta`), issue the `ping` command to the Tru64 UNIX system (`hostb`). The two systems should perform IKE negotiation and eventually communicate with each other using transport mode ESP protection. The successful display of the `ping` command output indicates this.

You can then issue the `netstat -x` and `netstat -X` commands to display the negotiated Security Associations (SAs) to verify that the correct SAs have been created. Also, the `/var/adm/syslog.dated/current/auth.log` file shows the log messages that are generated by the IPsec subsystem.

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

## Troubleshooting

If you determine that this Best Practice was not successful, as described in *Verifying Success*, see the problem solving section of the *Network Administration: Connections* manual for Tru64 UNIX problems and the appropriate Microsoft Windows 2000 documentation for Windows 2000 problems.

## Alternative Practices

Although this Best Practice is the recommended method for implementing IPsec connections with Windows 2000 peers, if your system does not meet the requirements described in *Is This Best Practice Right for You?*, you can use alternative methods.

If you do not need to secure all IP traffic between two systems, you might want to use Secure Shell software or Secure Socket Layer (SSL). See the *Security Administration* manual for more information on these technologies.

## Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

[best\\_practices@zk3.dec.com](mailto:best_practices@zk3.dec.com)

## Legal Notice

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation in the United States and/or other countries. UNIX® is a trademark of The Open Group in the United States and/or other countries. All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq Computer Corporation, a wholly owned subsidiary of Hewlett-Packard Company, required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

None of Compaq, HP, or any of their subsidiaries shall be liable for technical or editorial errors or omissions contained herein. The information

is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP or Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.