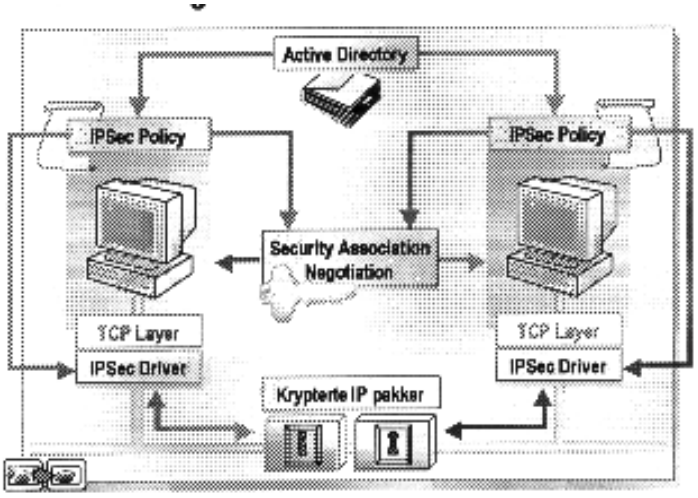
Konfigurering Netværk
Sikkerhed brugen af IPSec.

Indeholder

Introduktion til IPSec.

- Identificere sikkerhedstrusler i netværk.
  Hovedsagelige angreb på netværket:
  Overvågning af netværkstrafik (sniffer).
  Password (stjålet password, bryde/knække password).
  Adresse forfalske afsender adresse.
  Udnytte svagheder i netværksapplikationer (web, mail).
  Manden i midten (overvåger, opfanger eller kontrollere data mellem to parter, uden at de er klar over det).
  Denial-of-service (strømning).

- Hvad er IPSec godt for.



Implementering af IPSec.

- Aktivering af IPSec.
- Konfigurere IPSec for sikkerhed mellem maskiner.
- Konfigurere IPSec for sikkerhed mellem netværk.
- Tilpasse IPSec Policies.
- Valg af kryptering.
- Test af IPSec Policy.
- Optimalisering af IPSec ydelse.

Aktivering af IPSec.

- Console Windows Help
- Action View Favorites
- Tree Favorites Name Description Policy Assigned

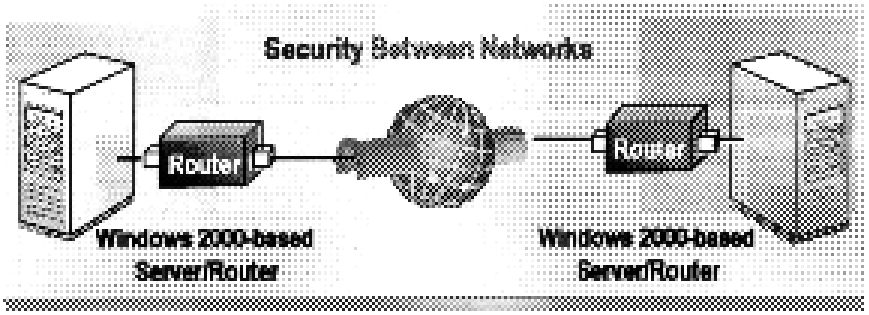
❖ Console Root
  - ➢ IP Security Policies on Local Machine
    - Client (Respond Only) Communicate normally (unsecured… No
    - Server (Request Security) For all IP traffic, always request… No
    - Secure Server (Require Sec… For all IP traffic, always require … Yes

Konfigurere IPSec for sikkerhed mellem maskiner.

- Brug af IPSec i Transport Mode.
- Påtvinger IPSec Policies for udveksling mellem systemer.
- Støtter Windows 2000.
- Giver ende til ende sikkerhed.
- Er default for IpSec.

Konfigurere IPSec for sikkerhed mellem netværk.

- Brug af IPSec i Tunnel Mode.
- Påtvinger IPSec Policies for at Internet trafik.
- Støtter også gamle OS
- Gir Point to Point sikkerhed.
- Endepunkt på ruterne.
- Slipper for at konfigurere hver klient.



Tilpasse IPSec Policies.

Regel komponenter.

- Tunnel Endepoint.
- Netværks type.
- IP filter list.
- Filter Action

Default Respons regler.

Test af IPSec Policy

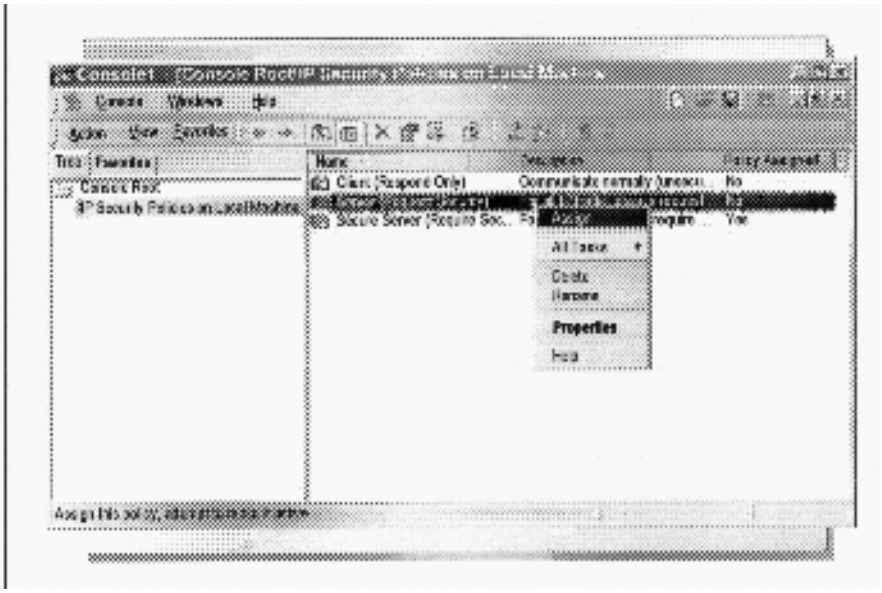
- Brug ping kommandoen til at identificere kontakt.
- Brug IPSec Monitor til at identificere at en Policy er blevet tildelt.

Optimalisering af IPSec ydelse.

For at sikre gennemstrømning, så tænk på:

-
- Hvilket niveau at sikkerhed er påkrævet.
- Sikkerhedskrav på maskiner.
- Antal IPSec Policy Filter poster.

Konfiguration TCP/IP for server sikkerhed.



Fejlsøgning af netværksprotokol sikkerhed.

Tjek system og sikkerheds logg for fejlmeldinger.
Tjek at en Security Association findes mellem maskiner.
Tjek at en Policy bruges på begge maskiner.
Tjek at en Policy er kompatibel med hinanden.
Tjek at alle ændringer er aktiveret.

Opsummering

- Introduktion til IPSec.
- Implementering af IPSec.
- Konfiguration af IPSec.
- Fejlsøgning.

Q. What is IPSec?

A. TCP/IP is widely used in most networks and with Windows 2000 forms a compulsory part of your network however a number of problems with TCP/IP exist.

Data is not sent in an encrypted format over TCP/IP, which leaves it vulnerable to a number of attacks including eavesdropping, which is where an attacker has access to the network, and can therefore view all data sent.

Being able to view data sent over the network would allow data such as passwords to be viewed when connecting to some services like FTP, which does not encrypt passwords sent over the network.

A solution was created in IPSec which is an industry standard based on end-to-end security which only the transmitting and receiving computers need know about any encryption.

Windows 2000 provides an implementation of IPSec and Group Policy settings in which to define your environments implementation of the IP add-on. Microsoft and Cisco developed this.

One of the great things with IPSec is it operates at layer 3 so any application of IP and upper layer protocols such as TCP, UDP will gain the advantage of IPSec without any modifications being needed to the applications.

Q. How can I restart the IPSec policy agent on a machine?

A. A. The policy agent is the component of Windows 2000 responsible for the negotiation between machines of the IPSec to use. If you experience problems and wish to restart to the agent you can stop and restart its service as follows:

C:\> net stop policyagent
C:\> net start policyagent

Q. How do I enable debug logging for IPSec?
A. **A.** Its possible to enable logging for IPSec which will result in logs being written to the %systemroot%\debug\oakley.log by performing the following registry change:

1. Start the registry editor (regedit.exe)
2. Move to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
3. From the Edit menu select New - Key
4. Enter a name of Oakley and click OK
5. Select the Oakley key and select New - DWORD value from the Edit menu
6. Enter a name of EnableLogging
7. Double click the new value and set to 1
8. Close the registry editor

Restart the policy agent

```
C:\> net stop policyagent
C:\> net start policyagent
```

Q. How do I enable IPSec traffic through a firewall?
A. IPSec is generally invisible to routers since it operates at layer 3 of the OSI layer an dall IP and upper-layer protocols are encrypted.
There is however a requirement for firewalls/gateways in the data path as the following IP protocols and UDP ports must be forwarded and not blocked for IPSec to correctly work.

- IP Protocol ID 50 - This is used for both inbound and outbound filters and is needed for Encapsulating Security Protocol (ESP) traffic to be forwarded
- IP Protocol ID 51 - As above but used for Authentication Header (AH)

traffic

- UDP Port 500 - For both inbound and outbound filters and needs to allow ISAKMP (Internet Security Association and Key Management Protocol) traffic to be forwarded

L2TP (layer 2 tunneling protocol)/IPSec traffic looks the same as just IPSec traffic on the wire and you need to open IP Protocol ID 50 and UDP Port 500.

Q. How can I troubleshoot IPSec?

A. There are a number of tools available to help you troubleshoot your IPSec configuration which consist of

The IPSec snap-in for policy configuration
The event log
Group Policy snap-in to set IPSec policies for a GPO
The file oakley.log in the %systemroot%\debug directory
But we will concentrate on two other tools, netdiag.exe and IPSecmon.exe.

IPSecmon.exe is part of standard Windows 2000 but netdiag.exe is supplied as part of the support tools (<CD:>\Support\Tools) so you will need to install these.

IPSecmon.exe is the simplest tool and shows current security associations for the hosts communicated with over IP and if IPSec is being used (and if it is what TYPE of IPSec).

Clicking the Options button allows the update frequency to be changed. In the example I have one IPSec association in place using Triple DES.

The meaning of each field is as follows:

Active Associations The number of active security associations with the computer being monitored.
Confidential Bytes Sent The total number of bytes sent with Confidentiality, indicating that the packets were sent using the Encapsulating Security Payload (ESP) security protocol (decimal ID 50).
Confidential Bytes Received The total number of bytes received with Confidentiality, indicating that the packets were sent using the Encapsulating Security Payload (ESP) security protocol (decimal ID 50).
Authenticated Bytes Sent The total number of bytes sent with the authentication property enabled.
Authenticated Bytes Received The total number of bytes received with the authentication property enabled.
Bad SPI Packets The total number of packets for which the Security Parameters Index (SPI) was invalid. This probably indicates that the security association (SA) has expired or is no longer valid.
The SPI is a unique identifying value in the SA that allows the receiving computer to select the SA under which a packet will be processed.
Packets Not Decrypted The total number of packets the receiving IPSec driver was unable to decrypt. This may indicate that the security association (SA) has expired or is no longer valid, authentication did not succeed, or integrity checking did not succeed.
Packets not authenticated the total number of packets that could not be successfully authenticated to the IPSec driver. This may indicate that the security association (SA) has expired or is no longer valid. The information in the security association is required for the IPSec driver to process the packets.
It may also indicate that the two computers have incompatible authentication settings. Verify that the authentication method specified for each computer is the same.
Key Additions The total number of keys that ISAKMP (the ISAKMP/Oakley mechanism) sent to the IPSec driver. This indicates that the ISAKMP Phase II security associations were successfully negotiated.
Oakley Main Modes the total number of successful security associations established during ISAKMP Phase I. This indicates that the key information exchange was successful. Identities were authenticated and common keying material was established.
Oakley Quick Modes the total number of successful security associations established during ISAKMP Phase II. This indicates that the negotiation for protection services during the data transfer was successful.
Soft Associations the total number of ISAKMP Phase II negotiations that resulted in the computers agreeing only to a clear-text data transfer (no encryption or signing of the packets).
Authentication Failures the total number of times authentication of the computer identities did not succeed. Verify that the authentication method settings for each computer are compatible. This may also indicate that the security association has expired.

Netdiag.exe is a more generic tool that is used to troubleshoot network connectivity problems but one of its options is to test IPSec as follows:

C:\>netdiag /test:ipsec /v /debug

Gathering IPX configuration information.
Opening \Device\NwlnkIpx failed
Querying status of the Netcard drivers... Passed
Testing Domain membership... Passed
Gathering NetBT configuration information.
Gathering IP Security information

Tests complete.

Computer Name: CYPHER
DNS Host Name: cypher.savilltech.com
DNS Domain Name: savilltech.com
System info : Windows 2000 Professional (Build 2195)
Processor : x86 Family 6 Model 5 Stepping 2, GenuineIntel
Hotfixes :
Installed? Name
Yes Q147222
Yes Q253562
Yes Q253934

Netcard queries test . . . . . : Passed

Information of Netcard drivers:

Description: Compaq NC3161 Fast Ethernet NIC
Device: \DEVICE\{9C65E63C-5242-45F8-9685-4A6649E92F35}

Media State: Connected

Device State: Connected
Connect Time: 16:34:16
Media Speed: 10 Mbps

Packets Sent: 25960
Bytes Sent (Optional): 0

Packets Received: 150278
Directed Pkts Recd (Optional): 32265
Bytes Received (Optional): 0
Directed Bytes Recd (Optional): 0

[PASS] - At least one netcard is in the 'Connected' state.

Per interface results:

Adapter : Local Area Connection
Adapter ID . . . . . : {9C65E63C-5242-45F8-9685-4A6649E92F35}

Netcard queries test . . . : Passed

Global results:

Domain membership test . . . . . : Passed
Machine is a . . . . . : Member Workstation

Netbios Domain name. . . . . : SAVILLTECH
Dns domain name. . . . . : savilltech.com
Dns forest name. . . . . : savilltech.com
Domain Guid. . . . . : {A225B0B5-8E82-4690-93F2-AA166BFDA773}
Domain Sid . . . . . : S-1-5-21-1614895754-1767777339-1801674531
Logon User . . . . . : Administrator
Logon Domain . . . . . : CYPHER

NetBT transports test. . . . . : Passed
List of NetBt transports currently configured:
NetBT_Tcpip_{9C65E63C-5242-45F8-9685-4A6649E92F35}
1 NetBt transport currently configured.

IP Security test . . . . . : Passed
Directory IPSec Policy Active: 'Server (Request Security)'

IP Security Verbose Test . . . . . : Failed
Access is denied.

The command completed successfully

Q. How can I disable IP Security (IPSec) on a VPN connection that uses Layer 2 Tunneling Protocol (L2TP)?
A. Windows automatically creates an IPSec policy for L2TP connections because L2TP doesn't encrypt data. However, you might want to test a VPN L2TP connection without the security of IPSec (e.g., when troubleshooting). Although you must disable IPSec on both the client and server in this situation, make sure you re-enable the security policy after you resolve any problems; otherwise, your systems are vulnerable to attack. To disable IPSec, perform the following steps on both ends of the connection (client and server):

9. Start a registry editor (e.g., regedit.exe).
10. Navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters subkey.
11. From the Edit menu, select New, DWORD Value.
12. Enter a name of ProhibitIpSec and press Enter.
13. Double-click the new value, set it to 1, and click OK.
14. Restart the machine.

For more information, see the Microsoft article "How to Configure a L2TP/IPSec Connection Using

Q. How can I manage/create IP Security policies?

A. Windows 2000 supplies the IP Security Policies MMC snap-in which can be used to modify and create IPSec policies which can then be assigned to computers and Group Policy Objects.

To open the snap-in perform the following:

Start the MMC (Start - Run - MMC.EXE)
From the console menu select 'Add/Remove Snap-in' (or press Ctrl+M)
From the Standalone tab click Add
Select 'IP Security Policy Management' snap-in and click Add
Select either 'Local computer' or the domain policy and click Finish. If its for a domain select 'Manage domain policy for this computer's domain'. Click Finish
Click Close to the dialog then click OK
Double clicking the root will display the 3 built-in options

Client (Respond Only)
Secure Server (Require Security)

Server (Request Security)
If you right click on the root you can create a new policy by selecting 'Create IP Security Policy'. If you right click on an existing policy and select Properties you can modify its settings.