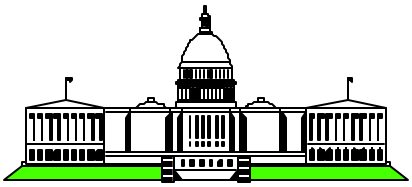
OS/390 Firewall Technologies
Virtual Private Network



Washington System Center

Objectives

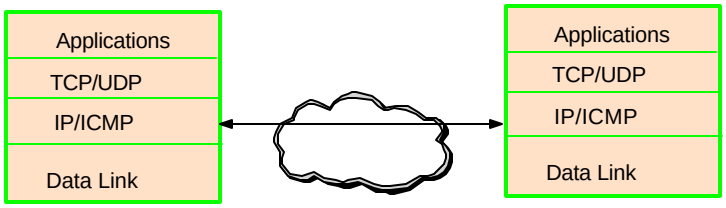
WSC Advanced Technical Support

- Overview of Virtual Private Networks
- IPSec
- Tunnel Security
- AH and ESP Headers
- Operation
- Tunnel Types and Modes
- Configuration
- IPSec Client

IPSec Overview

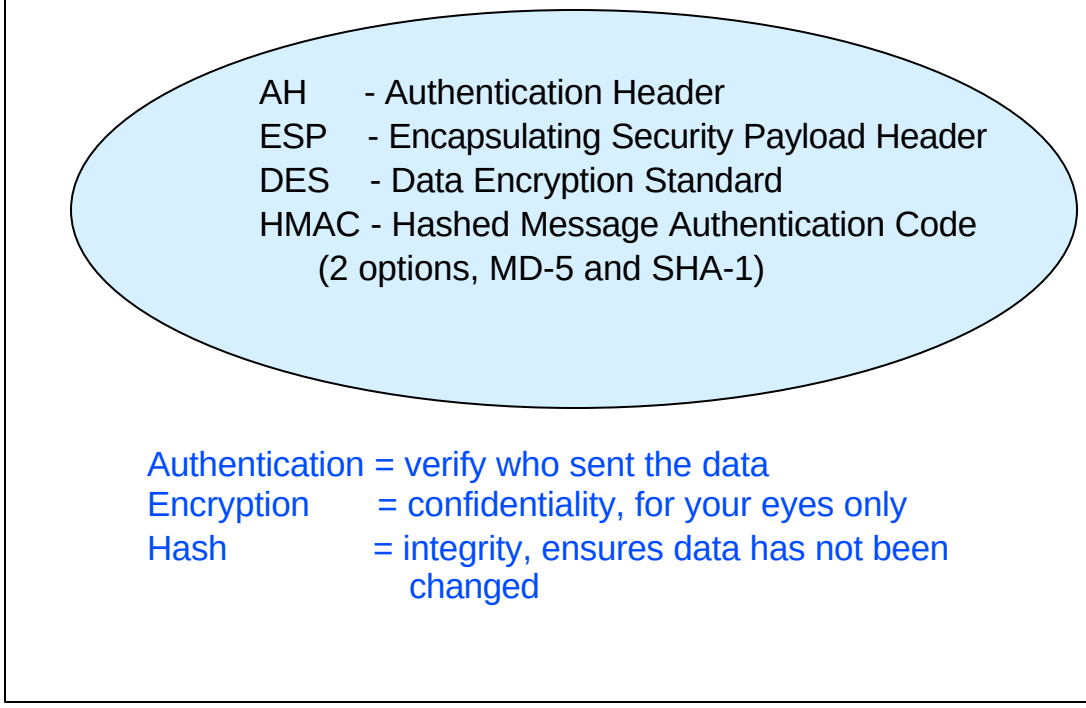
WSC Advanced Technical Support

- Open network layer security protocol endorsed by IETF
- Provides authentication, integrity and data privacy
  - packets are protected from snooping or modification
- Allows a secure tunnel between any two IP entities
- Management of crypto keys and security associations can be
  - manual
  - automated via key management protocol (IKE)
- Use of IPSec is transparent to upper layers including application



- Overall architecture of IPSec details are located in Request for Comment (RFC) 1825 and 2401.
- IETF - Internet Engineering Task Force
- S/390 Firewall Technologies 2.7 tunnel capability only supports manual keys. 2.8 l supports automatic key management.

IPSec Protocols and Algorithms



- Details for AH and ESP are located in RFC 1826 - 1829 and the latest is located in RFC 2402 - 2406 and 2410.

Tunnel Security

WSC Advanced Technical Support

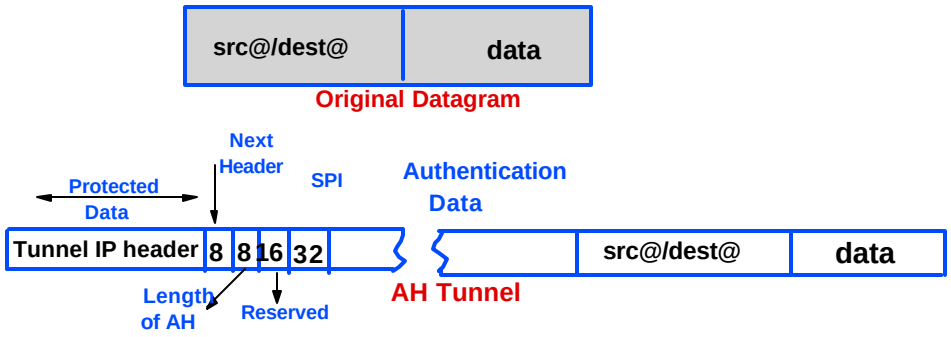
The VPN defined policy specifies that the data (original IP packet) be either:

(**encr**) encrypted
(**auth**) authenticated
(**ae**) authenticated after encrypting
(**be**) authenticated before encrypting

IPSec Objectives	Primary Protocol
Data Origin Authentication	AH
Data Integrity	AH
Data Confidentiality	ESP
Replay Protection	AH, ESP

Authentication Header (AH)

- Provides integrity-checking information and validates sender
  - detects if packet's contents were forged or modified when transmitted across untrusted networks
  - contains a cryptographic checksum to verify that the packet contents were not changed
  - Checksum computations will fail if packet contents are tampered with
    - incorporates secret keying information
    - prevents an attacker from computing an alternative checksum that checks correctly

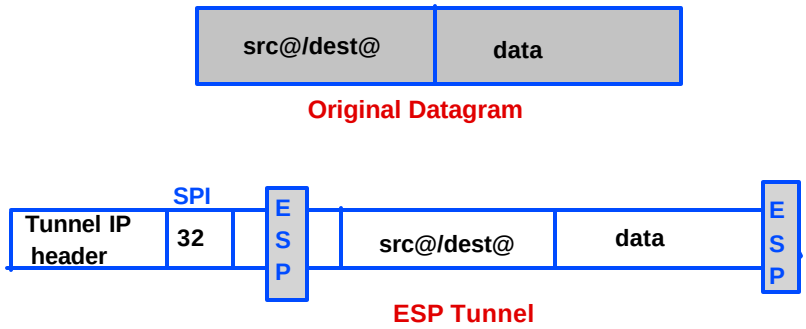


- The IPSec AH header is an IP packet that contains a cryptographic checksum for the packet's contents.
- AH is inserted into the packet between the IP headers and any subsequent packet contents.
- SPI - Security Parameter Index is a numerical value that is used by hosts processing IPSec . The SPI identifies the crypto keys and procedures to use with the SPI.
- AH header format;
  > first word identifies the type and location of the next protocol header
  > the SPI tells the destination host which security association applies to this header
  > rest of header is a multiple of 32-bit words that contains the cryptographic checksum

Encapsulating Security Payload (ESP)

WSC Advanced Technical Support

- Encrypts the data contents of the remainder of the packet
  - contents cannot be extracted while transmitted over nonsecure networks
  - format of ESP varies according to;
    - type of encryption
    - mode of encryption
  - SPI is associated with crypto keys used



- IPSec ESP processing includes transforming the protected data into an unreadable, encrypted form.
- The ESP consists of a 32-bit SPI field, followed by data with a format that depends on the encryption procedure being used. ESP incorporates all remaining data in the packet (any embedded headers or other fields, will not be processed until they have been decrypted at the receiving end).

Security Associations in IPSec

WSC Advanced Technical Support

- Hosts using IPSec must establish a *security association* with one another
  - Security Association establishes the what and how of IPSec protection
    - what types of protection to apply
    - how to do encryption or authentication
    - which keys need to be used
- Security association that applies to a IPSec header is;
  - determined by the packet's destination IP address
  - SPI in the packet header

- For each SPI IPSec software maintains;
  > crypto methods to be used by a specific SPI
  > keys to be used by the crypto methods when processing traffic for a specific SPI
  > the hosts or other entities associated with this traffic

- When IPSec protection is applied to an outgoing packet, it uses a security association belonging to the destination. The sending system applies the association's crypto method and key to the data to protect it, and inserts the association's SPI in the IPSec header.

- When a system processes the first IPSec header in an incoming packet, the SPI is used to identify that appropriate security association. The processing system applies the indicated crypto method to the header using the indicated key.

- If a header's SPI doesn't exist or the packet is invalid after processing, it is silently discarded. No indication is given to the sending host that the packet was rejected.

Operation of VPN

WSC Advanced Technical Support

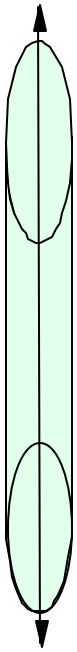
- The secure VPN relies on symmetric-key cryptography to enforce data security
  - firewalls at each end of the tunnel have a shared secret key
    - encryption key known to both firewalls
  - secret key provides two different types of security;
    - integrity - firewall appends message authentication code (MAC) to the data it sends through the tunnel
      > MAC is constructed from the data contents and the encryption key using a one-way hash function
      > receiving firewall performs the same operation, if MAC matches, the message is authenticated
    - privacy in which the data within the message is encrypted using the secure key, so that it can not be viewed in transit

- Symmetric Key - both sites have and use the same key
- Firewall takes message and secret key, runs it through an algorithm and creates the MAC.
- Hashing is a type of checksum and prevents anyone from seeing the original text.
- Authentication and encryption can be used independently. Each tunnel may utilize different features.
- Multiple tunnels may exist between the same nodes which might be useful for different encryption and authentication choices.

Types of Tunnels

WSC Advanced Technical Support

- Three types of tunnels;
  - IBM tunnel which is used between two IBM Firewalls and features an automatic key refresh mechanism
    - new encryption keys are generated at regular intervals and communicated through the tunnel under the current key
  - Manual tunnel that uses the IPSec standard and can be established between an OS/390 Firewall and;
    - any IPSec compliant firewall
    - an AIX IPSec client
    - an AIX 4.3 TCP/IP stack which has IPSec support
    - Windows 95 client running E-Network Communication Suite for Windows V1.0
  - A dynamic tunnel
    - uses IPSec standard
    - used between an AIX Firewall & Windows 95 secure remote client
    - configured but not activated until the remote client activates the tunnel



- E-Network Communication Suite for Windows V1.0 was tested with OS/390 Firewall Technologies.
- AIX IPSec client is supplied with IBM Firewall 3.1 for AIX. A IPSec client can establish a manual tunnel with any IPSec compliant host.
- Manual tunnels currently do not support any key refresh mechanism. When using a manual tunnel, it is necessary to inhibit key updates.

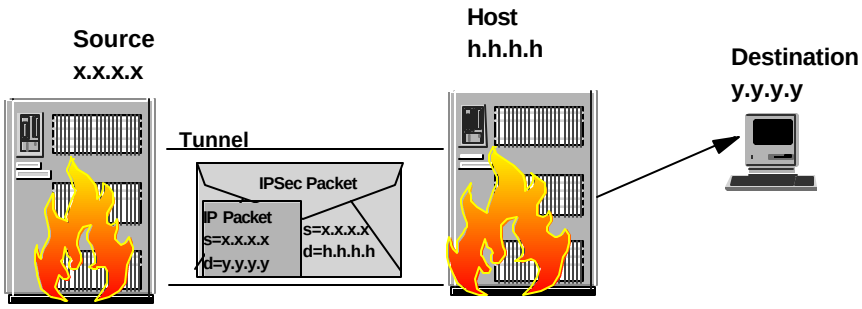
VPN Supports

WSC Advanced Technical Support

- VPN provided by OS/390 Firewall Technologies only supports manual tunnels
  - default tunnel life is 480 minutes (8 hours)
  - maximum time 44640 minutes (31 days)
  - secure IP tunnel will need to be refreshed on a regular basis
    - if key updates are required a secure method must be devised for transporting the keys to the destination system

Manual Tunnel

- Typically used for security associated between two Firewalls
  - may be used between;
    - two IPSec compliant firewalls
    - a IPSec compliant firewall and a IPSec Client

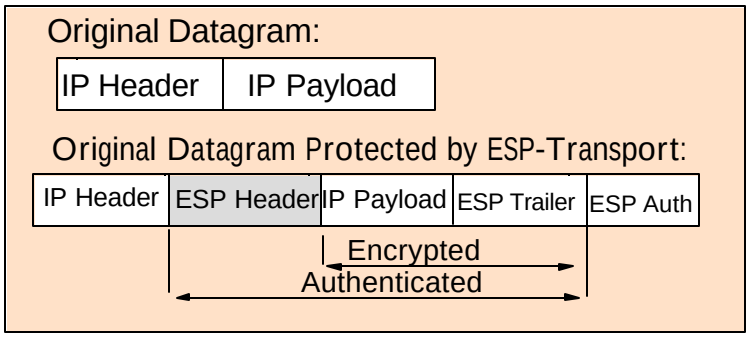


source and destination addresses in the new IP header are the addresses of the tunnel's endpoints

- A tunnel protects the entire IP packet by enclosing it within an IPSec packet.
- New IP header is attached at the beginning of the IPSec packet to form a new IP packet.
- Source and destination may be different from the enclosed packet.

Transport Mode

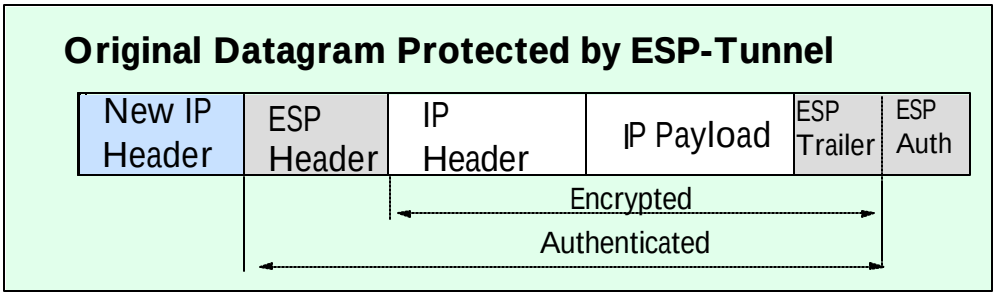
Protects IP Data, but not the Headers.
Origin's & Recipient's IP Addresses in the clear.

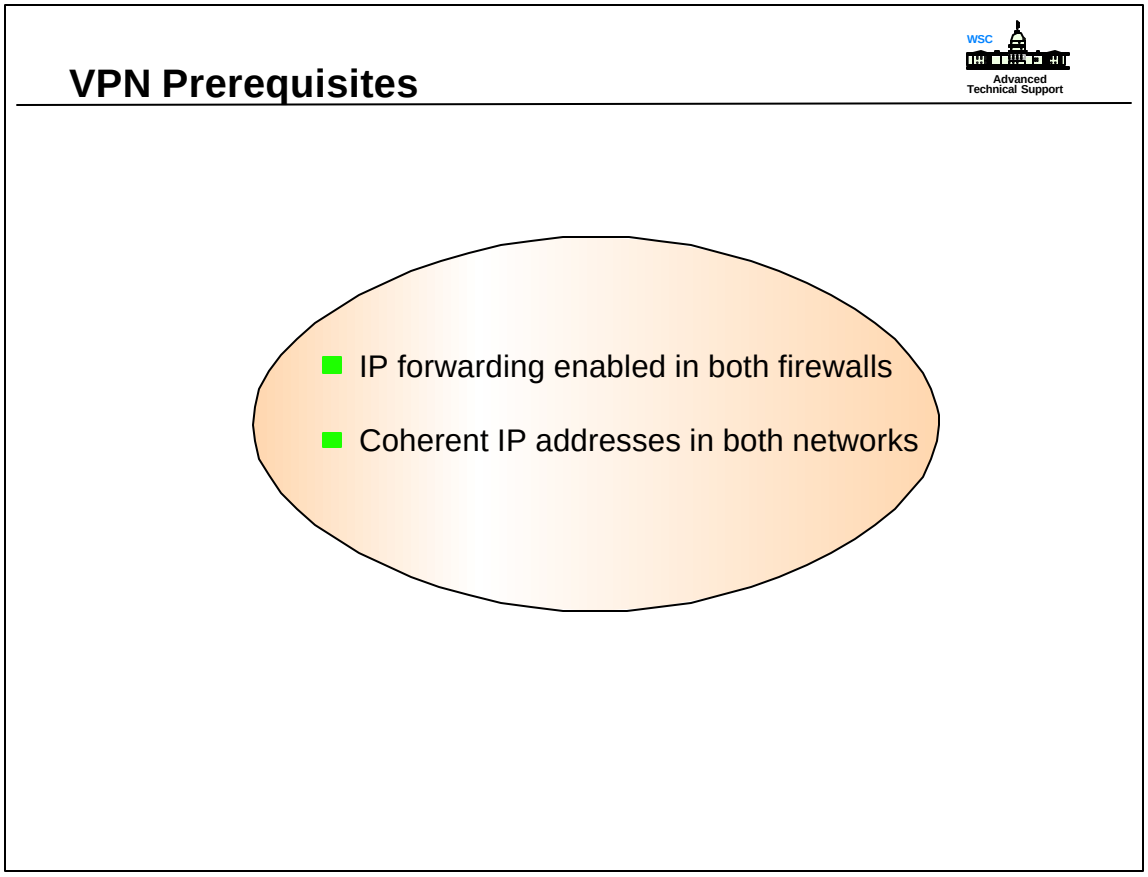


- Transport tunnels - protects only the transport-layer packet (UDP or TCP) inside an IP packet
- IP protocol header is separated from the transport-layer packet
- Transport-layer packet is enclosed in an IPSec packet
- IP header is attached to the IPSec packet, forming new IP packet length, protocol and header checksum fields in the IP header are modified accordingly

Tunnel Mode

Protects Entire Packet:
Original IP Data,
Original IP Headers,
ESP Header





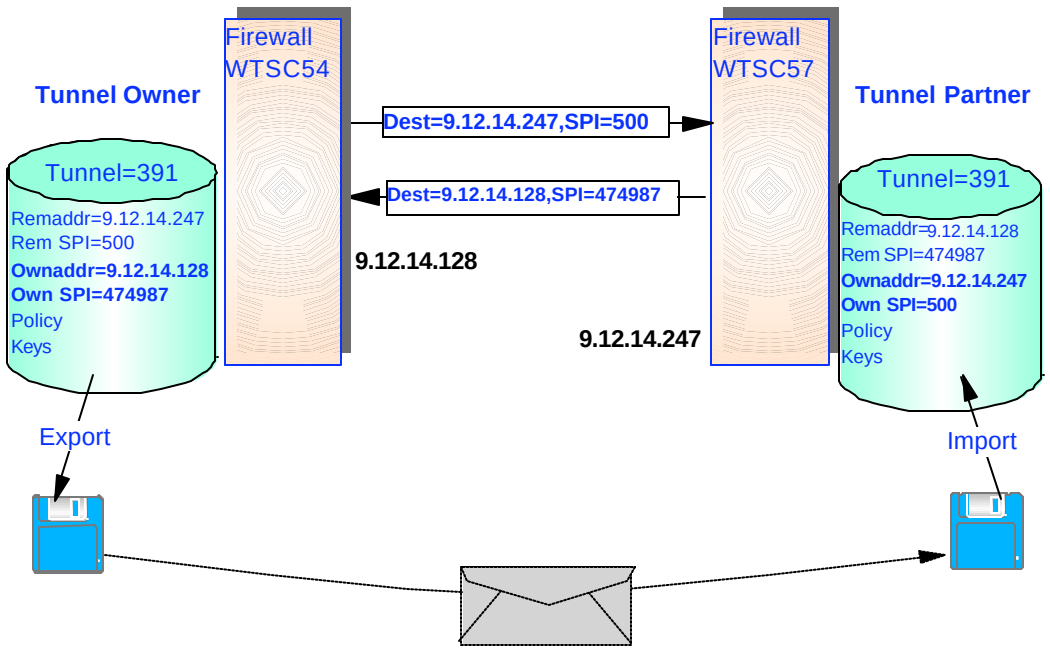
- IP forwarding is determined in the TCP/IP profile. If the profile has the parameter NOFWD specified, it must be removed. IP forwarding is the default.
- IP Forwarding is handled by routers. The router will process each IP datagram separately. A packet traveling through the Internet will be forwarded by several routers until it reaches it's final destination.

VPN Configuration

WSC Advanced Technical Support

- To configure tunnels;
  - Local Host
    1. create firewall network objects
    2. add tunnel definition
    3. export the tunnel definition to a set of files
    4. transfer the tunnel definition files to the partner tunnel
    5. define filter rules and services for VPN
    6. add connection definitions
  - Remote Host
    7. import the tunnel definition in the remote firewall
    8. repeat 1,5,6 at remote firewall
  - Both Hosts
    9. activate rulesets at both ends
    10. activate tunnel at both ends
    11. refresh the tunnel when session key has expired

Tunnel Security Association



Network Objects

- **WTSC54 (local host)**
  - **fwnwobj cmd=add name=localhost desc="S/390 Local Host WTSC54" type=host addr=9.12.14.128 mask=255.255.255.255**
  - **fwnwobj cmd=add name=remotehost desc="Remote Host WTSC57" type=host addr=9.12.14.247 mask=255.255.255.255**

- Network objects define the address for the endpoints of the tunnel and the type.
- IP tunnels are secure logical connections between two machines. They provide security in the form of authentication and encryption for the data passing through them. This requires that machines at each end of the tunnel share a secret key

Tunnel Definition

WSC Advanced Technical Support

```
fwtunnl cmd=add tunnel=391 type=manual addr=9.12.14.128
        remaddr=9.12.14.247 policy=auth algorithm=KEYED_MD5
        spi=500 timeout=480
```

>tunnel = numeric tunnel ID (1 - 999999)
>type = type of tunnel, OS/390 only supports manual
>addr = IP address of the local firewall machine
>remaddr = IP address of the tunnel target (tunnel partner)
>policy = specify combination of encryption and authentication values
>encrypthow = encryption method to use (optional when POLICY=AUTH is used)
>algorithm = authentication algorithm to use, OS/390 only supports KEYED_MD5
>spi = used to index to the correct encryption and/or authentication technique combination for the tunnel
>timeout = life span of the tunnel, default 480 minutes (8 hours), max 44640 minutes (31 days)

- OS/390 Firewall Technologies will use hardware encryption services if available, if not the processing will be performed in software.

- Policy allowed;
  > authenticate after encrypting
  > authenticate before encrypting
  > authenticate
  > encrypt

- Authenticate after encrypting: authentication header protocol is seen so filter rules for AH are needed.

- Authenticate before encryption: encryption header protocol is seen so filter rules for ESP are needed.

- Encryption methods allowed are;
  > CDMF (masking)
  > DES 56 bit with 32 bit initialization vector
  > DES 56 bit with 64 bit initialization vector
  (DES option is valid only for the US and Canada)

Tunnel Definition .....

WSC Advanced Technical Support

fwtunnl cmd=add tunnel=391 ..... optional parameters

>**destpolicy** = default is value used in **policy**
>***destalgorithm*** = *specified if **destpolicy** is specified, default is value for* **algorithm**
>***destAHauthkey*** = *authenticationkey, specified if **destalgorithm** is specified*
>***destencrypthow*** = *default is value used in* **encrypthow**
>***destESPencrkey*** = *encryptionkey, specified if **destrncrypthow** is specified*
>**destAHspi** = default is value in **SPI**
>**destESPspi** = will use value in **SPI**
>**destESPauth** = default is value used in **algorithm**
>***destESPauthkey*** = *specified if **destESPauth** is specified*

- All of these parms are optional and in some cases when they are not specified the system will generated the needed value. This offers an advantage because some keys generated by humans are considered from a mathamatical viewpoint, to be weak keys.

- These options provide the tunnel partners more options. One partner may want to send everything encrypted when the other partner may only want or need to send data authentication.

Tunnel Definition .....

WSC Advanced Technical Support

fwtunnl cmd=add tunnel=391 ..... optional parameters

>**srcAHspi** = value in **srcESPspi** is used if not specified

>**srcESPspi** = if not specified a system generated value is assigned

>**srcAHauthkey** = if not specified a system generated key is assigned, works with **algorithm**

>**srcESPencrkey** = if not specified a system generated value is assigned, works with **encrypthow**

>**srcESPauth** = ESP authentication algorithm

>***srcESPauthkey*** = *specified if **srcESPauth** is used, else a system generated key is used*

Tunnel Definition .....

WSC Advanced Technical Support

fwtunnl cmd=add tunnel=391 ..... optional parameters

>**newheader** = specifies what RFCs the AH and ESP headers conform to
yes = RFCs 2401-2406 and 2410
no = RFCs 1825-1829
default depends on tunnel algorithms specified

>**replay** = monitors incoming IP packets to ensure that the system does not receive identical or old packets. Valid only when new header format is specified

>**mode** = operational mode of the tunnel (transport or tunnel), default is tunnel

Tunnel Command Examples

WSC Advanced Technical Support

- Change addr, remaddr, policy, encrypthow, algorithm, spi, and timeout may be changed

```
fwtunnl cmd=change tunnel=391 addr=9.12.14.127 remaddr=9.12.14.246
policy=encr encrypthow=des_CBC_4 spi=502 timeout=360
```

- Activate/deactivate specify one or more tunnels to be activated or all tunnels

```
fwtunnl cmd=activate or deactivate tunnel=(tunnel_id1, tunnel_id2)
```

- Delete tunnels specified by one or more tunnel IDs

```
fwtunnl cmd=delete tunnel=tunnel_id1
```

- Export creates files to be exported to partner tunnel

```
fwtunnl cmd=export directory=directory or tunnel=tunnel_id1
```

- Import creates files that contain exported partner tunnel definitions

```
fwtunnl cmd=import directory=directory or tunnel=tunnel_id1
```

- Deactivate stops all tunnel activity

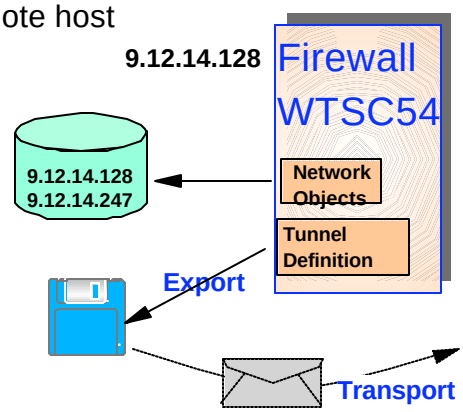
```
fwtunnl cmd=deactivate tunnel=tunnel_id1
```

- When commands are entered they could be in a shell script which could be executed or if they are entered from the command line in OMVS use the '\' continuation character if command is too long to fit on one line.

- For examples of shell scripts reference the appendix in the OS/390 Firewall redbook.

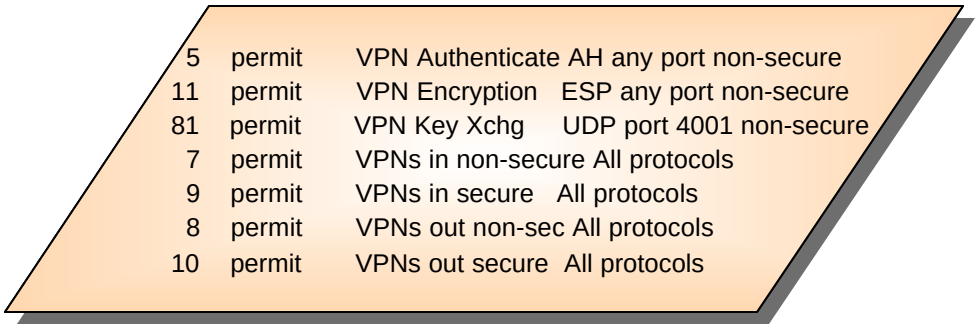
Export

- Tunnel definition must be exported to a format that may be transported to the remote site for importing into the partner firewall
  - **fwtunnl cmd=export directory /anyexportdirectoryname tunnel=391**
- Command creates two files in /anyexportdirectoryname called **fwexppolicy** and **fwexpmctx.manual**
- Transport files to remote host



- When doing the export the tunnel number must be specified and it should be the same number used in the Tunnel definition command.
- Sending the export file should be done with care since the files contain the secret keys that will be shared between the tunnel partners.
- If a secure method exist to transmit the files (e.g. encryption) you may choose to use that method. Or installations may choose to copy the files to some media (disk, tape, etc) and have it delivered.

VPN Default Rules



- These are the default rules supplied with Firewall Technologies that a customer may want to use. The defaults can be used, or a customer may want to recreate a default rule if they want to turn logging on. These rules do not have to be used, a customer may create the filter rules that fit their environment.

Tunnel Filter Rules

WSC Advanced Technical Support

- Tunnel Filter Rules
  - same as normal rules
  - rules also contain tunnel ID
- Rules for
  - requesting all traffic flow through tunnel xx
  - ESP, encrypted packets
  - AH, authenticated packets

- Tunnel rules are like regular filter rules in that they both contain source, target, protocol, ports and port operations. A tunnel rule will also contain a tunnel ID. When a packet is transferred, the OS/390 Firewall Technologies will search the filter rules, if one matches and this rule has a tunnel ID, the packet will be sent according to the authentication/encryption rules specified in this specific tunnel.

- The filter rules must be defined in both tunnel partners.

Tunnel Rule and Service Definition

WSC Advanced Technical Support

- Rule (WTSC54, 9.12.14.128)
  - **fwfrule cmd=add type=permit name=tunneltraffic desc="route all traffic" protocol=all srcopcode=any srcport=0 destopcode=any destport=0 interface=nonsecure routing=local direction=both log=no tunnel=391**
  - **fwfrule cmd=add type=permit name=ahtraffic desc="authenticated traffic" protocol=ah srcopcode=any srcport=0 destopcode=any destport=0 interface=nonsecure routing=local direction=both log=yes**
- Service (WTSC54, 9.12.14.128)
  - **fwservice cmd=create name=alltrafficservice desc="all traffic" rulelist=505/f,505/b,504/f,504/b**

- Assume the rule for requesting all traffic flow through tunnel **391** was given **ID 504** and the authentication rule was given **ID 505** on system **WTSC54**.
- The order of the filter rules is important, the rules associated with the IPSec protocol should always be placed at the beginning of the list. Use fwservice cmd=move to arrange the order of rules.

Encryption

WSC Advanced Technical Support

- **fwfrule cmd=add type=permit name=vpnen desc=encryption protocol=esp srcopcode=any srcport=0 destopcode=any destport=0 interface=nonsecure routing=local direction=both log=yes fragment=yes**
- **fwservice cmd=create name=vpnencaps desc="encryption traffic" rulelist=506/f,506/b**

► If encryption was used, both systems would require a rule to handle encrypted traffic. Assuming the system generated ID 506 for the encryption rule, the encryption service would be defined associating the rule with the service.

Connections

WSC Advanced Technical Support

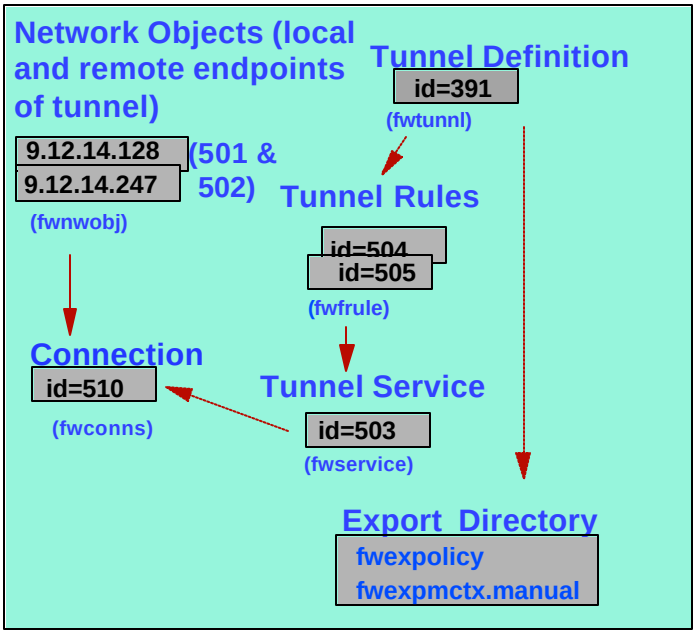
- Connection associates local and remote host network objects with filter rule services
  - **WTSC54**
    - **fwnwobj cmd=list**
      > id=501, type=host name=localhost desc="S/390/Local Host wtsc54" addr=9.12.14.128 mask=255.255.255.255
      > id=502, type=host name=remotehost desc="Remote Host wtsc57" addr=9.12.14.247 mask=255.255.255.255
    - **fwservice cmd=list id=503**
      > id=503, name=alltrafficservice desc=all traffic rulelist=504/f,504/b,505/f,505/b
  - **fwconns cmd=create name=alltrafficconnection source=501 destination=502 servicelist=503**

- By listing the network objects and services we find the ID numbers associated with the entries. The ID numbers are then used in the connection command and the system **WTSC54** has now completed it's tunnel setup.

Tunnel Review

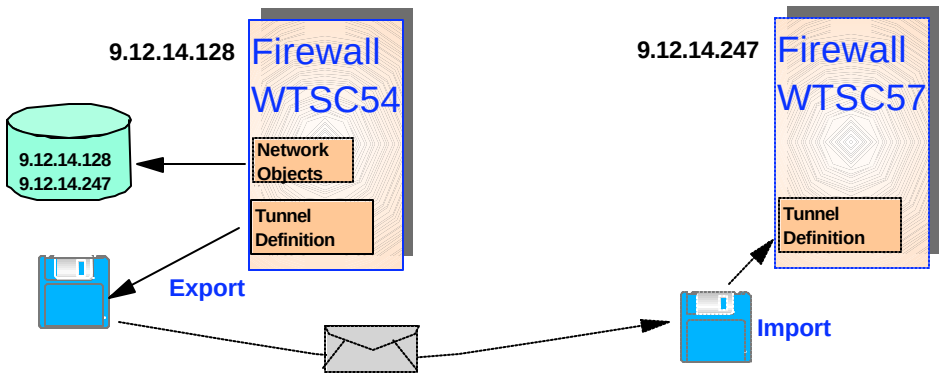
WSC Advanced Technical Support

G'Burg Firewall WTSC54 9.12.14.128



Receive and Import

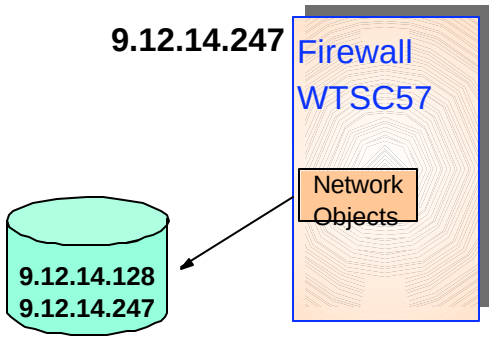
- Receive files sent from tunnel partner
- After tunnel partner receives the exported files, place them in a directory and import the definitions;
  - **fwtunnl cmd=import directory=/importdirectoryname tunnel=391**



- From system **WTSC57**, 9.12.14.247 receive the files and import them to a directory specifying the same tunnel ID that **WTSC54** used.
- If files are imported to an AIX firewall, rename the **fwexppolicy** file to **fwexppolicy.3.1**. If the definition was created on AIX and exported to OS/390 the file **fwexppolicy.3.1** has to be renamed to **fwexppolicy**.

Network Objects

- **WTSC57**
  - **fwnwobj cmd=add name=wtsc57 desc="wtsc57 system" type=host addr=9.12.14.247 mask=255.255.255.255**
  - **fwnwobj cmd=add name=wtsc54 desc="wtsc54 host" type=host addr=9.12.14.128 mask=255.255.255.255**



Tunnel and Service Examples

WSC Advanced Technical Support

- Filter Rule
  - WTSC57 9.12.14.247
    - **fwfrule cmd=add type=permit name=tunneltraffic desc="route all" protocol=all srcopcode=any srcport=0 destopcode=any destport=0 interface=nonsecure routing=local direction=both log=yes tunnel=391**
    - **fwfrule cmd=add type=permit name=vpn desc="authenticated traffic" protocol=ah srcopcode=any srcport=0 destopcode=any destport=0 interface=nonsecure routing=local direction=both log=yes fragment=yes**
- Service
  - WTSC57, 9.12.14.247
    - **fwservice cmd=create name=alltrafficservice desc="all traffic" rulelist=501/f,501/b**
    - **fwservice cmd=create name=vpnauth desc="authenticate traffic" rulelist=503/f,503/b**

- System **WTSC54 and WTSC57** now have rules that request all traffic flow through tunnel 391 and rules for handling authenticated traffic.

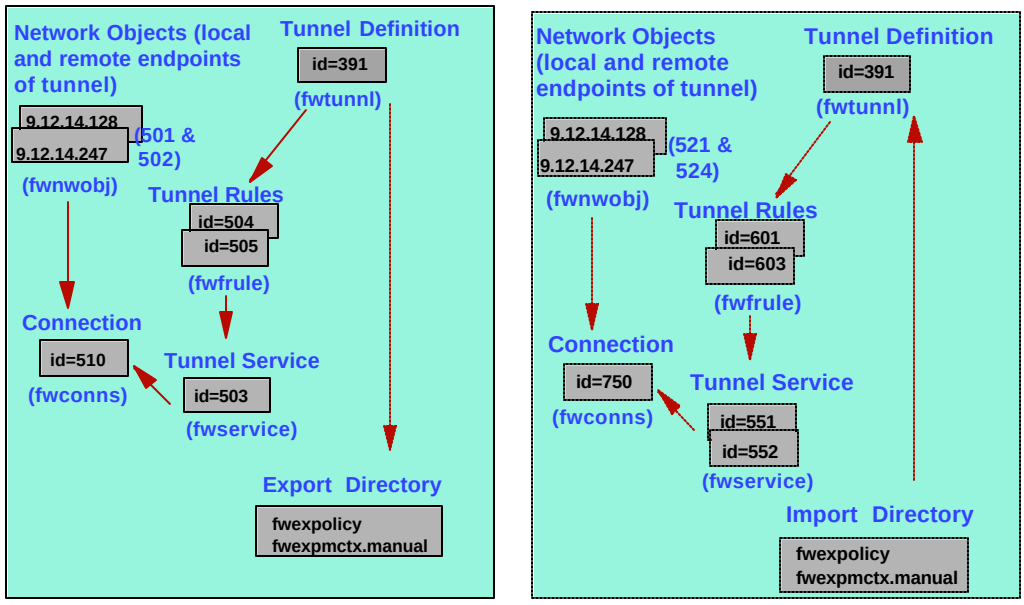
Connections

WSC Advanced Technical Support

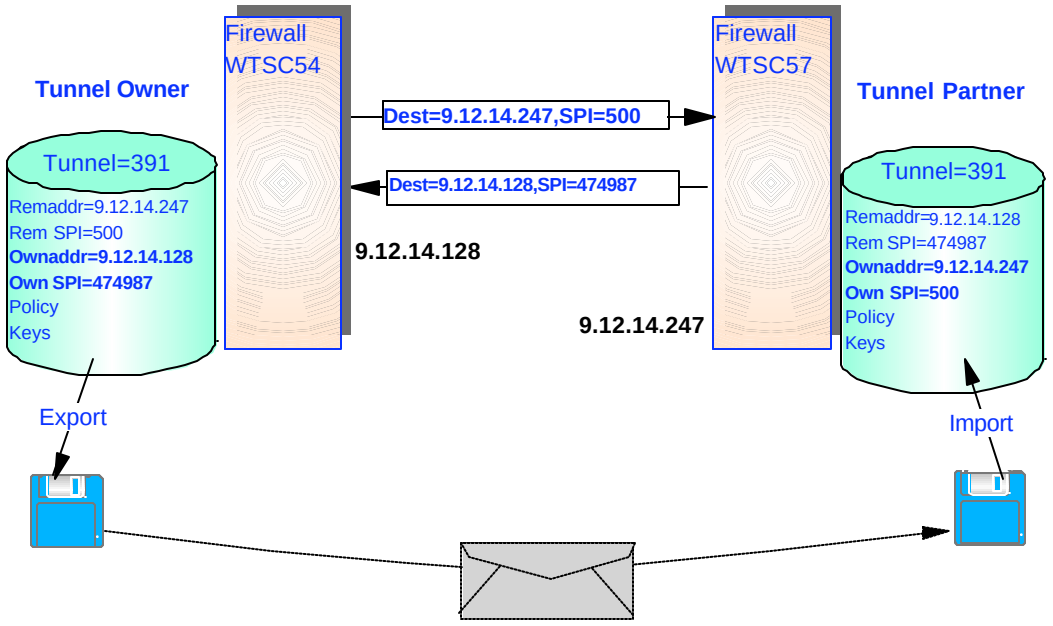
- **WTSC57**
  - **fwnwobj cmd=list**
    > id=521, type=host, name=wtsc57, desc="wtsc57 system"
    addr=9.12.14.247 mask=255.255.255.255
    > id=524, type=host, name=wtsc54, desc="wtsc54 host"
    addr=9.12.14.128 mask=255.255.255.255
  - **fwservice cmd=list**
    > id=551, name=alltrafficservice, desc=all traffic rulelist=601/f,601/b
    > id=552, name=vpnauth, desc=authenticate traffic, rulelist=603/f,603/b
  - **fwconns cmd=create name=alltrafficconnection desc="connect all traffic" source=521 destination=524 servicelist=551,552**

▶ **WTSC57** completes it's tunnel setup by entering the connection definitions.

Tunnel Review



Tunnel Security Association



Activate Rulelist and Tunnels

WSC Advanced Technical Support

- **fwfilter cmd=update**

  cmd=
  - update refreshes the IP filter rules file and activates them
  - verify check filter rule file for valid syntax and dependencies
  - list active filter and Socks rules in the filter rules files
  - shutdown deactivates all filter rules and prevents traffic from reaching the socks daemon
  - startlog starts logging of filters rules
  - stoplog stops logging of filter rules
  - listsocks list the socks rules in socks configuration file

- When both tunnel partners have the correct definitions, activate the tunnel
  - **fwtunnl cmd=activate tunnel=391**

    Tunnel activation enables the code and will be marked active even if the other end is not running or connected

- For the rules to take affect both tunnel partners must issue the **fwfilter cmd=update**.
- For logging to take place the log parameter must be set in the filter rules and started via the FWFILTER command.
- The configuration files should not be edited or the file may become corrupted. The Firewall commands can be used to change the contents of the configuration files.
- The configuration files were written in the IBM 1047 code page, which deals with code translation. If by chance the firewall is installed on a system that is not running in the IBM 1047 code page, the configuration files may become corrupted if they are edited. Many of the configuration files contain variant characters.

Activate & List Tunnel Definitions

WSC Advanced Technical Support

fwtunnl cmd=activate

- WTSC54
  - list tunnel
    - **fwtunnl cmd=list tunnel=391**

Results; tunnel = 391
state=Active
type = manual
addr = 9.12.14.128
remaddr = 9.12.14.247
policy = auth
encrypthow = CDMF
algorithm = KEYED_MD5
spi = 500
timeout = 480
Firewall SPI = 474987

fwtunnl cmd=activate

- WTSC57
  - List tunnel ID on partner system
    - **fwtunnl cmd=list tunnel=391**

Results; tunnel = 391
state=Active
type = manual
addr = 9.12.14.247
remaddr = 9.12.14.128
policy = auth
encrypthow = CDMF
algorithm = KEYED_MD5
spi = 474987
timeout = 480
Firewall SPI = 500

- When you list the tunnel there are two SPI numbers, the one entered in the tunnel definition and the FIREWALL SPI generated by the system. These numbers will be used in the partner tunnel firewall and they are used to identify the crypto keys and procedures to use with it.
- No validation of target addresses is done during import processing so ensure that the addressing is correct.

Refresh Tunnels

WSC Advanced Technical Support

- Tunnel will cease operation when tunnel lifetime is reached
- Tunnel Refresh
  - **fwtunnl cmd=activate**
  - keys remain the same

- The deactivate/activate could be setup in a REXX exec that is run every morning, or it could be setup in a CRON table. CRON tables can be schedule like jobs to kick off at specific times.

- Even if a tunnel has expired it must still be deactivated before it can be activated. When the tunnel expires the firewall TCP/IP stack recognizes it, the command portion does not. Therefore, the command deactivate must be done before an activate can be issued.

- If a tunnel has expired, and a deactivate has not be issued, the tunnel will still display it as active. Currently there are no means to find out if the TCP/IP stack has marked the tunnel as expired. If data attempts to pass through an expired tunnel, the data will be rejected and discarded.

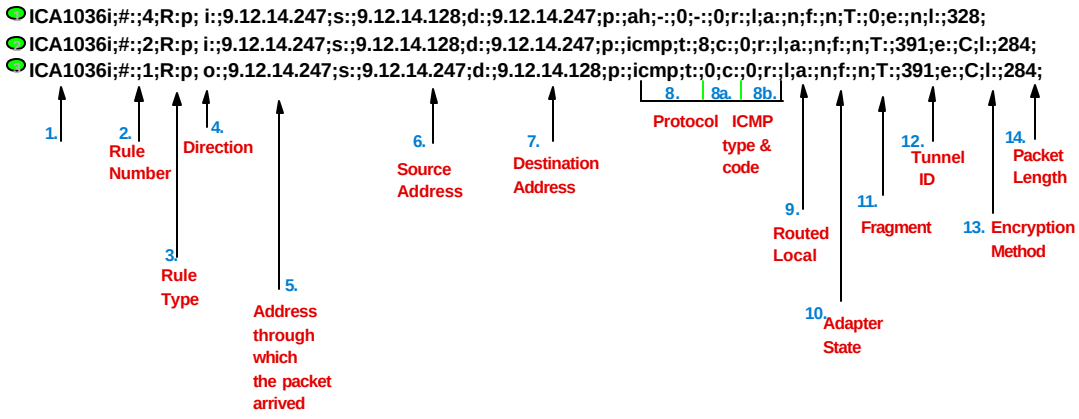
Refresh Tunnels....

WSC Advanced Technical Support

- Re-establish tunnel with new keys
  - remove tunnel parameter from rules
  - delete tunnel definition
  - add tunnel parameter to rules
  - add tunnel definition with same tunnel ID & characteristics
  - export
  - new session keys are stored inside the definition files
  - tunnel partner deletes tunnel parameter from rules
  - tunnel partner deletes existing tunnel
  - add tunnel parameter to rules
  - re-imports new tunnel definitions
  - activate rules and tunnel definitions in both systems

VPN Log

Line 1, is inbound AH (authenticate)
Line 2, is inbound ICMP decrypted
Line 3, is outbound ICMP response packet



- A simple way to check that the VPN tunnel is functioning is to perform a PING to the tunnel's partner. This is the log output from WTSC57 when a PING was done from WTSC54.

1. Message Number
2. #: - Rule number packet matched
3. R: - Rule Type p=permit, d=deny
4. Packet direction i=incoming, o=outgoing
5. Adapter Address through which packet arrived
6. s: - Packet source address
7. d: - Packet destination address
8. p: - Packet's protocol, 8a. ICMP type , 8b. ICMP code
9. r: - Packet's destination with respect to the firewall machine r=routed, l=local
10. .a: - Adapter state through which packet arrived s=secure, n=nonsecure
11. f: - Packet's fragmentation state, y=yes, n=no
12. T: - Tunnel number associated with packet
13. e: - Packet encryption method, n=none, C=CDMF, D=DES
14. l: - packet's length in bytes

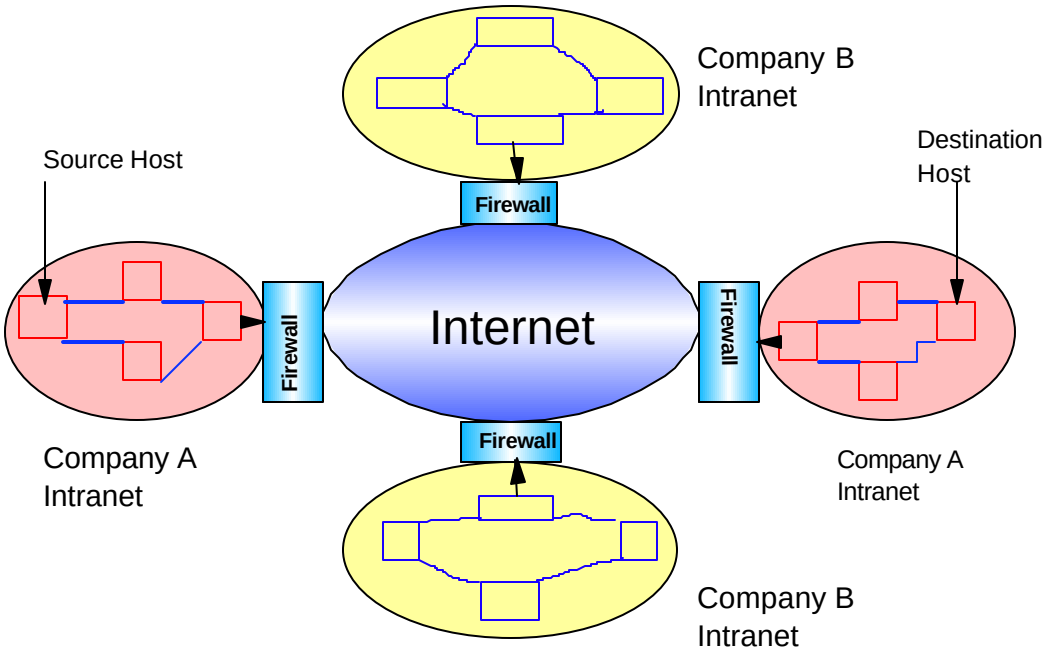
IPSec Client

WSC Advanced Technical Support

- IPSec client is supplied with IBM Firewall 3.1 for AIX
- IPSec client can communicate through a secure tunnel
- IPSec procedure is described in IBM Firewall for AIX User's Guide V3.1.1, GC31-8419-00
- Configuration steps for AIX IPSec client are very similar to the OS/390 Firewall Technologies secure tunnel implementation
  - add a tunnel on the AIX IPSec client machine
  - export the tunnel definition on the AIX IPSec client machine
  - transfer the tunnel definition to the tunnel partner
  - import the tunnel definition in the tunnel partner
  - activate the tunnel at both ends
  - refresh the tunnel when session key expires

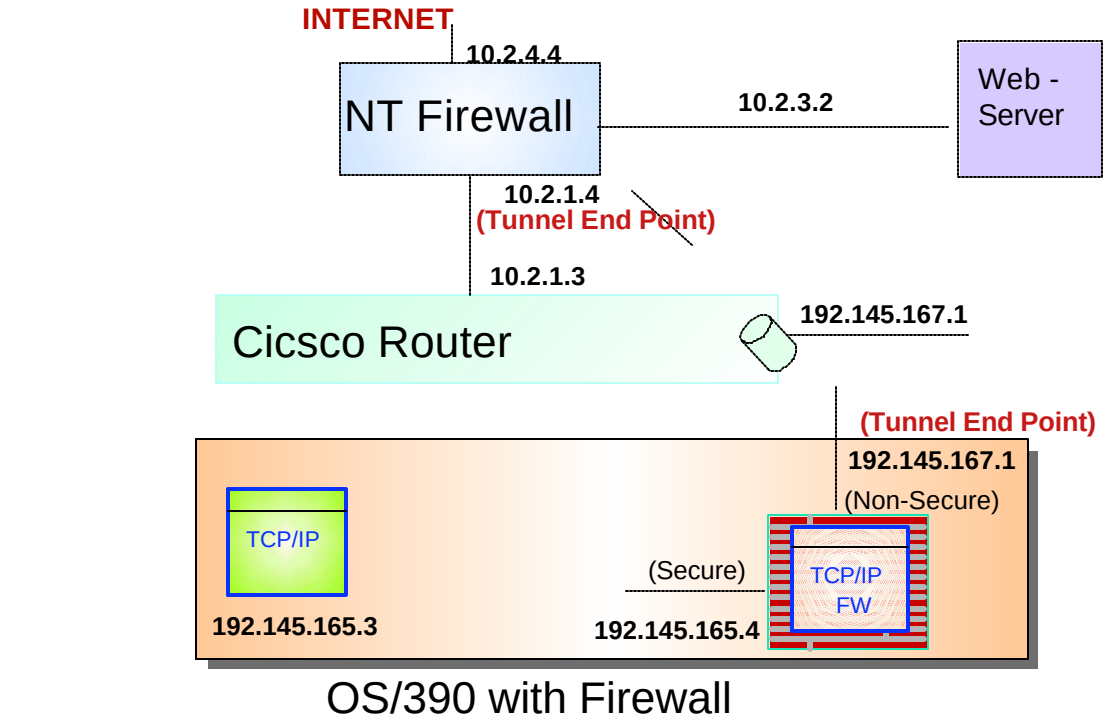
► The IBM redbook "Stay Cool on OS/390: Installing Firewall Technology", has examples of AIX screens for defining a tunnel on a AIX IPSec client.

Interconnecting Branch Offices



- Customers use VPNs to;
  1. interconnect branch offices
  2. interconnect with different companies intranets
  3. Dial in Remote Access
     For dial in remote access you need a dynamic key exchange protocol like ISAKMP/Oakley. which is used in S/390 Firewall 2.8.

Firewall/VPN Layout



Tunnel & Rules

WSC Advanced Technical Support

```
# fwtunnl cmd=list tunnel=10
        tunnel = 10
        state = Active
        type = manual
        addr = 192.168.164.1
        remaddr = 10.4.3.1
        encrypthow = DES_CBC_8
        policy = ae
        timeout = 44640
        spi = 500
        algorithm = KEYED_MD5

        Firewall SPI = 256
```

#:5 permit 192.168.166.1 255.255.255.255 10.4.1.2 255.255.255.255;all; any 0; any 0; both both both l=y f=y t=10 e=DES_CBC a=KEYED_MD5 p=n;

#:6 permit 10.4.1.2 255.255.255.255 192.168.166.1 255.255.255.255;all; any 0; any 0; both both both l=y f=y t=10 e=DES_CBC a=KEYED_MD5 p=n;

#:18 permit 10.4.3.1 255.255.255.255 192.168.164.1 255.255.255.255;ah; any 0; any 0; both both both l=y f=y t=0 e=none a=none p=n;

#:20 permit 10.4.3.1 255.255.255.255 192.168.164.1 255.255.255.255;all; any 0; any 0; both both both l=y f=y t=10 e=DES_CBC a=KEYED_MD5 p=n;

Log of Example Tunnel

Jul 26 13:25:32 DYATRON : 1999;00000024: 2073;ICA1036i;#:;21;R:p;
i:;192.145.165.4;s:;192.145.165.3;d:;10.2.3.2;p:;icmp;t:;8;c:;0;r:;r;a:;n;f:;n;T:;0;e:;n;l:;284;
Jul 26 13:25:32 DYATRON : 1999;00000024: 2073;ICA1036i;#:;5;R:p;
o:;192.145.167.1;s:;192.145.165.3;d:;10.4.1.2;p:;icmp;t:;8;c:;0;r:;r;a:;n;f:;n;T:;10;e:;D;l:;284;
Jul 26 13:25:32 DYATRON : 1999;00000024: 2073;ICA1036i;#:;18;R:p;
i:;192.145.167.1;s:;10.2.1.4;d:;192.145.167.1;p:;ah;-:;0;-:;0;r:;l;a:;n;f:;n;T:;0;e:;n;l:;344;
Jul 26 13:25:32 DYATRON : 1999;00000024: 2073;ICA1036i;#:;6;R:p;
i:;192.145.167.1;s:;10.2.3.2;d:;192.145.165.3;p:;icmp;t:;0;c:;0;r:;r;a:;n;f:;n;T:;10;e:;D;l:;284;
Jul 26 13:25:32 DYATRON : 1999;00000024: 2073;ICA1036i;#:;6;R:p;
o:;192.145.165.4;s:;10.2.3.2;d:;192.145.165.3;p:;icmp;t:;0;c:;0;r:;r;a:;n;f:;n;T:;10;e:;D;l:;284;
Jul 26 13:34:34 DYATRON : 1999;00000024: 2073;ICA1036i;#:;21;R:p;

Glossary

WSC Advanced Technical Support

- AH - Authentication Header, a protocol of IPsec
- DES - Data Encryption Standard
- ESP - Encapsulating Security Payload, a protocol of IPsec
- Encrypted Tunnels - secure, remote access
- FTP - File Transfer Protocol, developed/maintained by IETF
- GW - Gateway
- HMAC - Hashed Message Authentication Code
- IETF - Internet Engineering Task Force, develops technical standards for the InternetIP - Internet Protocol, developed/maintained by IETF
- IPSec - IP Security, developed/maintained by IETF
- L2TP - Layer 2 Tunnel Protocol (Cisco, Microsoft)
- MD-5 - Message Digest 5
- VPN - Virtual Private Network
- Tunnels - encapsulated traffic

Selected Bibliography

- SC24-5835 OS/390 Firewall Technologies Guide & Reference
- SG24-2046 Stay Cool on OS/390: Installing Firewall Technology
- (example of V2R5, Tunnel Mode, definition)
- SG24-2577 Implementing an IBM Internet Firewall/AIX
- (AIX & Windows clients; manual key mgt applies to S/390)
- GC31-8419 IBM Firewall for AIX User's Guide
- SG24-5201 (IBM) Comprehensive Guide to VPNs
- SG24-5227 eNetwork Comm.Server V2R5 TCP/IP: Config & Routing
- SG24-4986 Understanding LDAP
- SG24-4949 Security on the Web Using DCE Technology
- SG24-4803 How to Secure Internet Connect Server for MVS
- SR23-7296 Building Internet Firewalls; Chapman & Zwicky (O'Reilly)
- SR28-5580 Firewalls and Internet Security; Cheswick & Bellovin
- SR28-4970 DNS and BIND; Albitz & Liu (O'Reilly)
- GR19-5267 Internet Security Handbook; W. Stallings (McGraw-Hill)
- SR23-7375 Internet Security Professional Reference (New Riders)
- SG24-4564 www.security: How to Build a Secure WWW Connection
  - MacGregor, Aresi, Siegert (Prentice Hall)
- xxxx-xxxx Unix System Security: Guide for Users & Systems Administrators
  - D.Curry (Addison-Wesley)
- G321-5666 Catapults and Grappling Hooks: The Tools and Techniques
  - of Information Warfare (A.Boulanger)
- SR23-8260 Understanding Digital Signatures; Gail Grant (McGraw-Hill)

References

WSC Advanced Technical Support

- RFC's
  - 1825 Security Architecture for Internet Protocol
  - 1826 IP Authentication Header
  - 1827 IP Encapsulating Security Payload
  - 1828 IP Authentication Using Keyed MD5
  - 1829 The ESP DES_CBC Transform
  - 2401 Security Architecture for Internet Protocol
  - 2402 IP Authentication Header
  - 2403 HMAC-MD5-96 within ESP and AH
  - 2404 HMAC-SHA-1-96 within ESP and AH
  - 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
  - 2406 IP Encapsulating Security Payload
  - 2410 NULL Encryption Algorithm and Its Use With IPsec