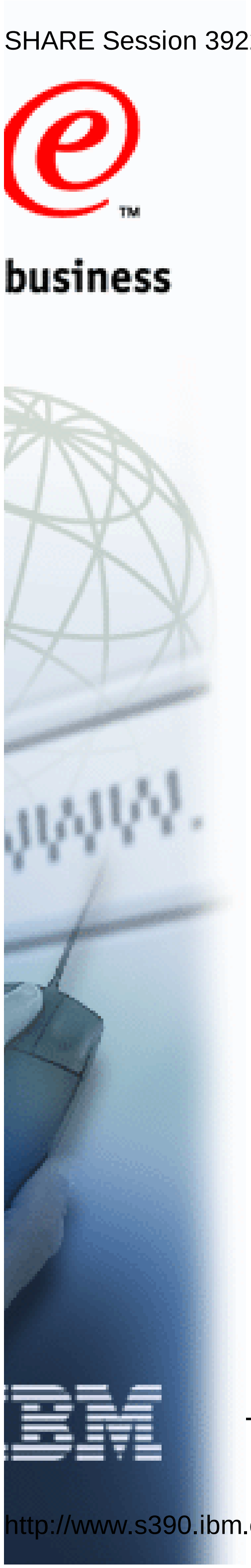


Getting Started: IPSec with CS for OS/390

SHARE Session 3922

July 25, 2000
Boston, Massachusetts

Dave Wierbowski
OS/390 Firewall Technologies Development
Endicott, New York

(607) 752-6739
wierbows@us.ibm.com

Trademarks

The following are trademarks of International Business Machines Corporation:

IBM
OS/390
RACF

The following are trademarks or registered trademarks of other companies or institutions:

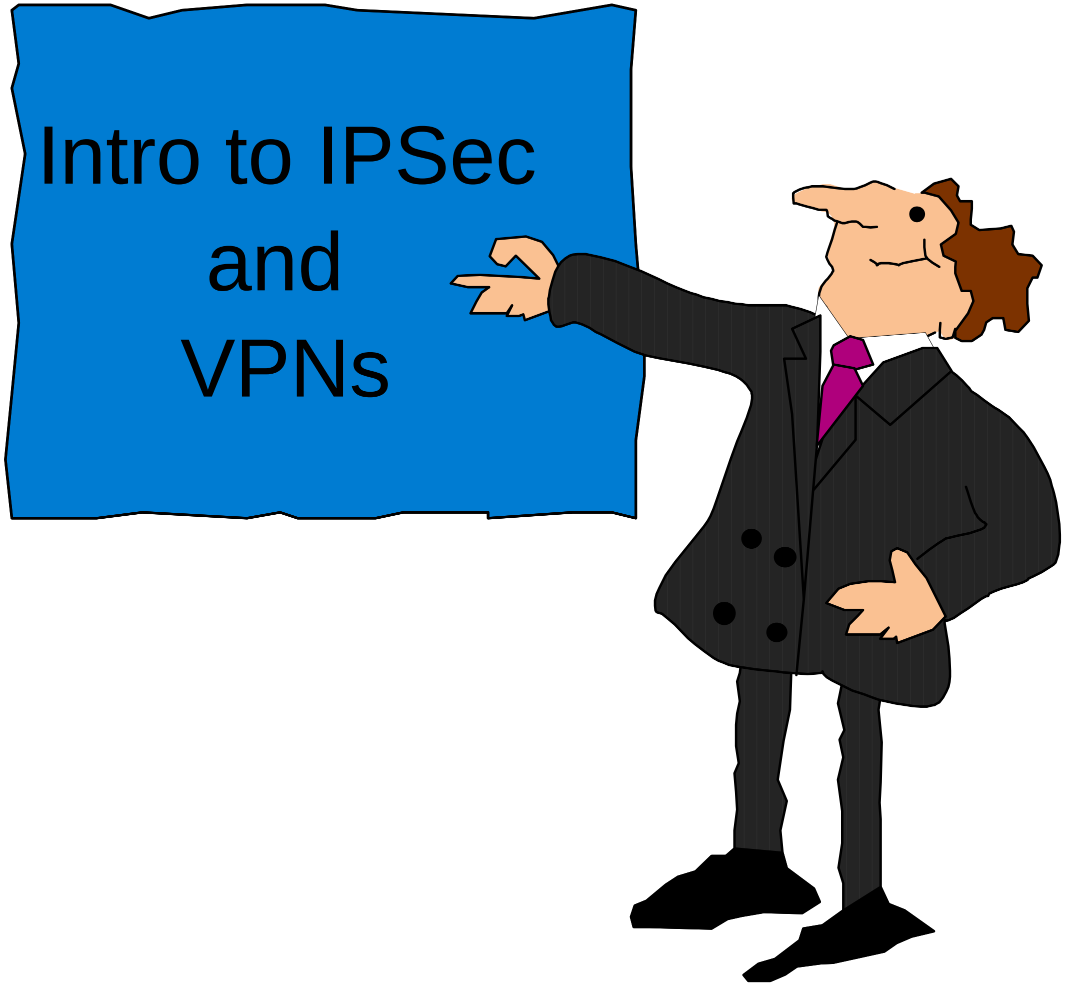
RSA

Abstract

"You've decided that you want to use the Communication Server on OS/390 to create an IPSec based VPN to protect your IP traffic. Now what? This session will discuss the pre-configuration steps of setting up your VPN. Specifically, it will discuss the information you will need to know along with the decisions you need to make before configuring your IPSec VPN on OS/390. It will include a walk-through of an example of gathering this information for a hypothetical VPN configuration. As part of this walk through you will be exposed to the various configuration objects that you will need to define when you configure your VPN."

Session objectives

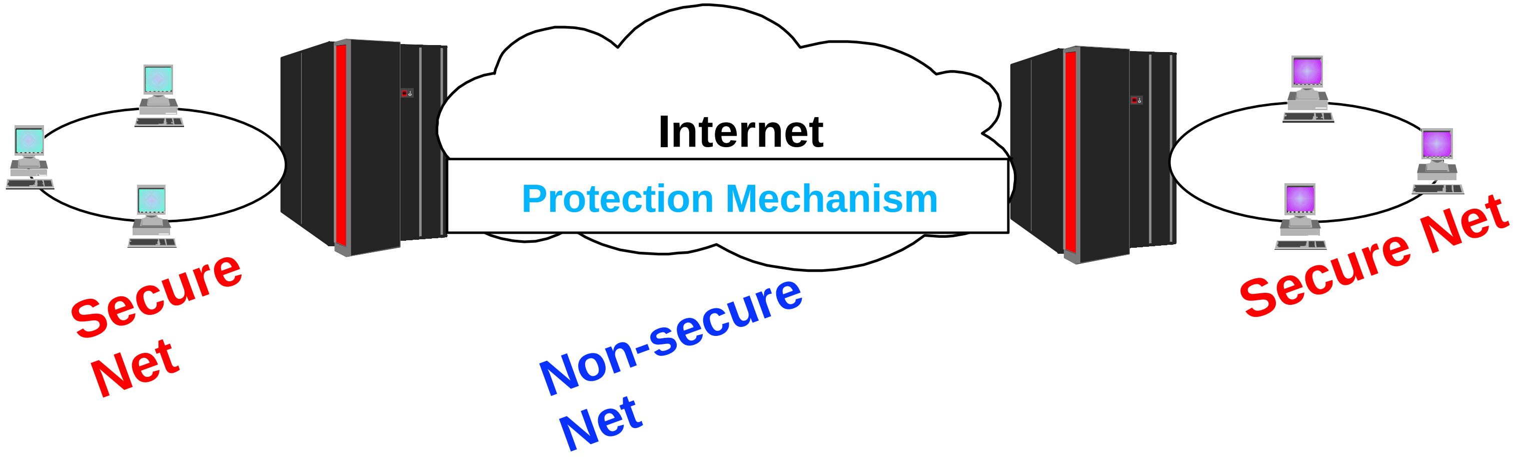
- □ Provide a brief introduction to VPNs and IPSec
- □ Identify many of the questions you need to answer before configuring an IPSec based VPN
- □ Provide insight into answering to these questions
- □ Walk-through examples of gathering this information
- □ Discuss how these questions relate to OS/390 VPN configuration
  - ● **Identify additional OS/390 VPN configuration issues**
- □ Provide a brief release by release summary of VPN support on OS/390



Intro to IPSec and VPNs

What is a VPN?

- A VPN is a:
  - **Virtual Private Network**
    - **Network**
      - **Two or more devices communicating with each other**
    - **Private**
      - **Confined to the members of the network**
    - **Virtual**
      - **Not really a private network, but has the essence of a private network**



- Something that provides security when two or more secure networks communicate across an unsecure network

Types of VPNs on OS/390

Manual VPNs

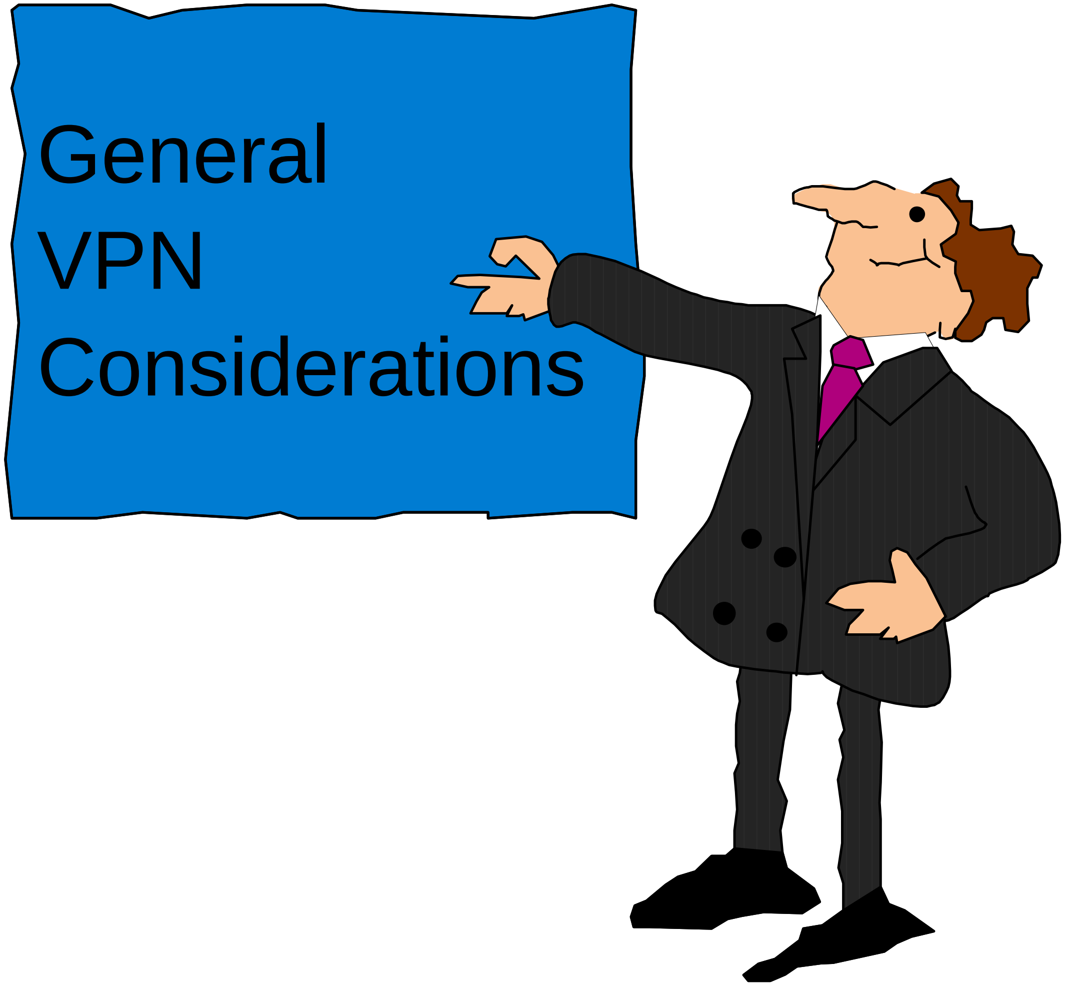
- VPNs whose attributes and encryption keys must be managed by administrative procedures
- First available via a kit in R4

Dynamic VPNs

- VPNs whose attributes and encryption keys are managed by the Internet Key Exchange (IKE) protocol
- First available in R8

What is IPSec?

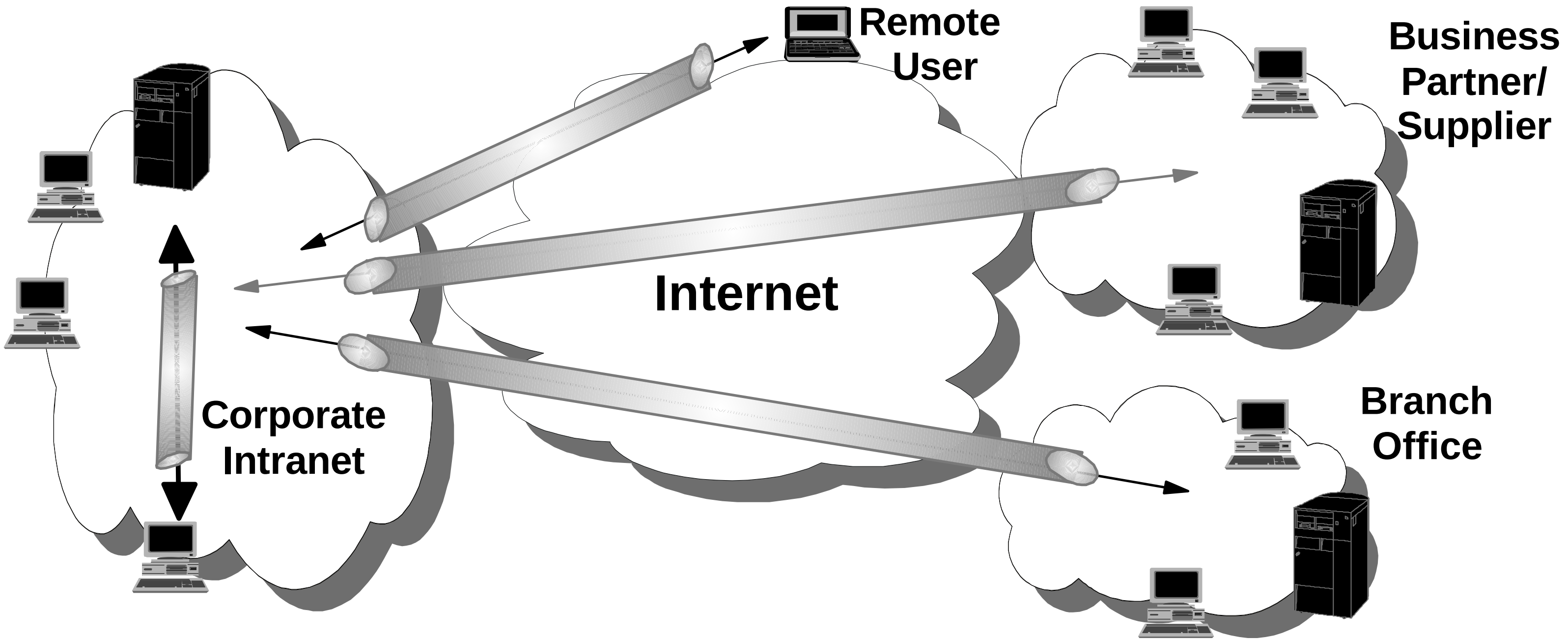
- A set of protection mechanisms (protocols) used to implement VPNs over IP based networks
  - **IP - Internet Protocol**
- Defined by the IETF’s IP Security Protocol Working Group (IPSec)
  - **IETF - Internet Engineering Task Force**
  - **IPSec - IP Security**
  - **A group whose purpose in life is to define standards pertaining to how to protect traffic in an IP based network**
- IPSec working group’s home page:
  - **http://www.ietf.org/html.charters/ipsec-charter.html**



General VPN Considerations

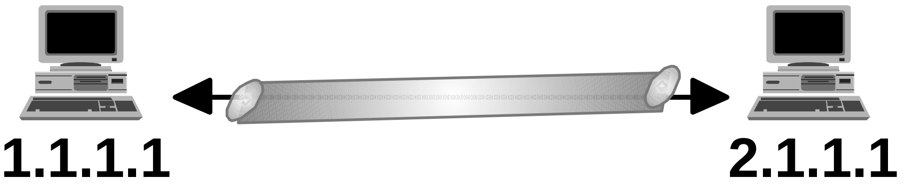
Where do I start?

- Figure out what traffic I need to protect
  - Do I have traffic I need to protect within my Corporate Intranet?
  - Do I have remote users that access my Corporate Intranet?
  - Do I have business partners or suppliers that I communicate with?
  - Do I have branch offices that I communicate with?
  - Do I need to protect this traffic with IPSec?



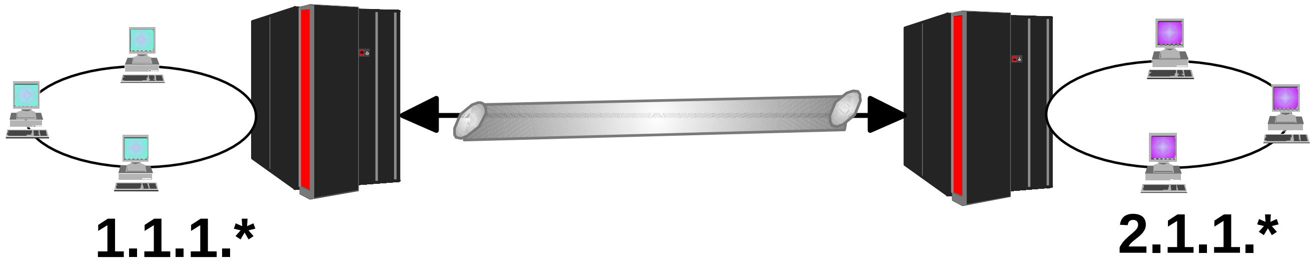
Where do I protect?

□ The entire communication path from host to host

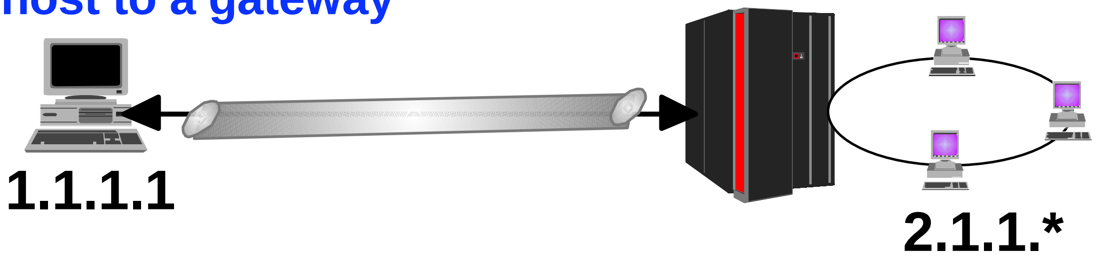


□ A subset of the communication path

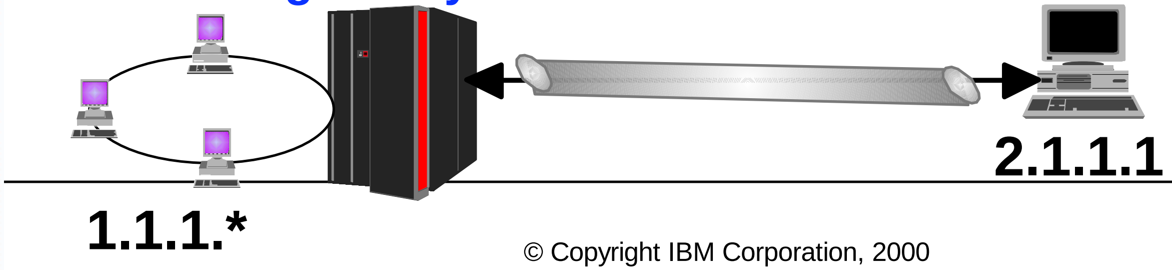
- From a gateway to another gateway (e.g. firewall to firewall)



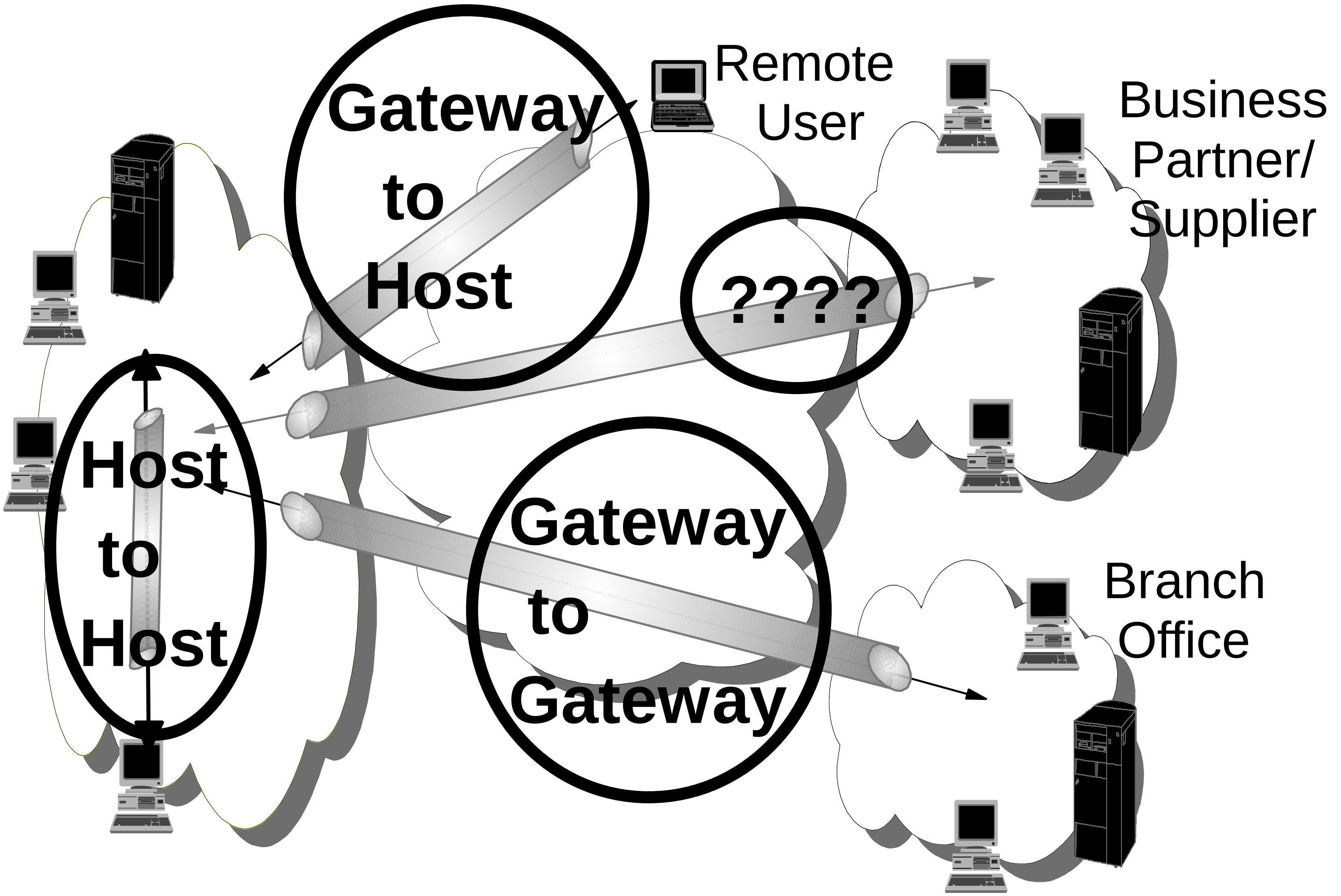
- From a host to a gateway



- From a gateway to a host



Where do I protect (continued)?



How do I want to protect data?

□ What are my options?

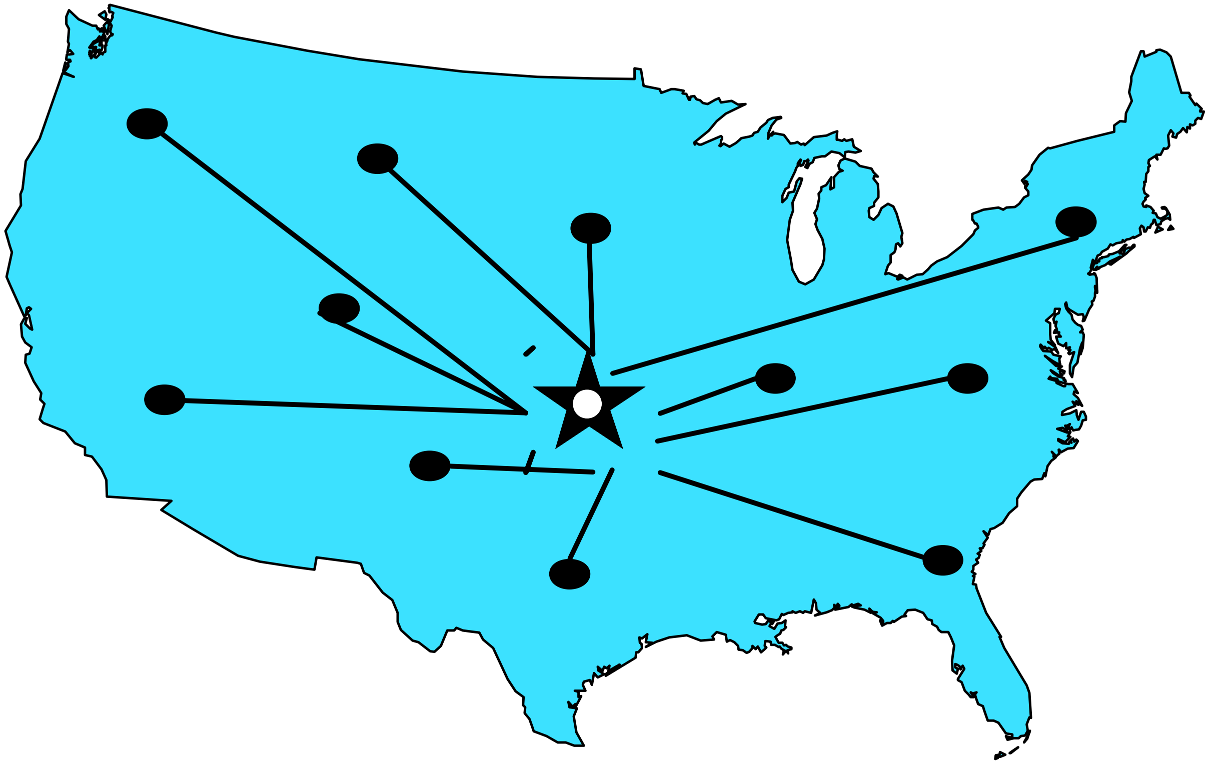
- IPSec's Authentication Header Protocol (AH) - RFC 2402
  - Obsoletes RFC 1826
- IPSec's Encapsulation Security Payload Protocol (ESP) - RFC 2406
  - Obsoletes RFC 1827

□ Which do I use?

- Do I need only data privacy?
  - Yes, then I must use the ESP Protocol
- Do I need only data integrity and/or data origin authentication?
  - Yes, then I can use either the AH Protocol or the ESP Protocol with NULL encryption
    - AH will authenticate selected fields of the IP header
    - ESP will not authenticate any fields of the IP header
- What if I need all three?
  - I would use the ESP Protocol
  - Alternatively, I could use AH for data integrity/authentication and ESP for data privacy

Why would I only want authentication?

- □ You don't care about privacy, but do care about who is communicating with you
- □ Example
  - ● **Meteorological monitoring devices reporting back to a central database**



Why mention obsolete RFCs?

- □ You need to be aware that there exists multiple versions of the AH and ESP protocols
  - ● They are not compatible
  - ● You might still encounter platforms that implement the obsolete RFCs
    - – OS/390 R5 and R6
- □ Can I still use the obsolete RFC?
  - ● Yes
- □ Why would I want to use an obsolete RFC?
  - ● Because you've you wish to create a VPN with a platform that only supports the old RFCs
    - – OS/390 R7 and R8 still supports these old RFCs for compatibility with R5 and R6

What parameters apply to AH and ESP?

	AH	ESP
Authentication Algorithm	X	X
Encryption Algorithm		X
Encapsulation Mode	X	X

What authentication algorithm can I use?

	Manual VPNs (Old RFCs)	Manual VPNs (New RFCs)	Dynamic VPNs
HMAC-MD5		X	X
HMAC-SHA		X	X
KEYED-MD5	X		

What encryption algorithms can I use?

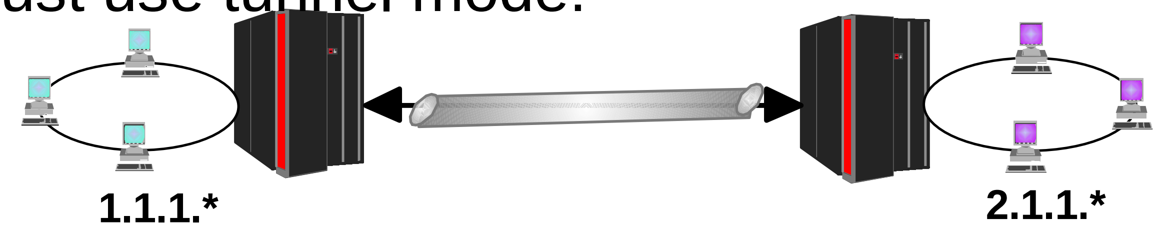
	Manual VPNs (Old RFCs)	Manual VPNs (New RFCs)	Dynamic VPNs
CDMF	X	X	
DES_CBC_4	X	X	
DES_CBC_8	X	X	X
3DES_CBC		X	X
ESP_NULL		X	X

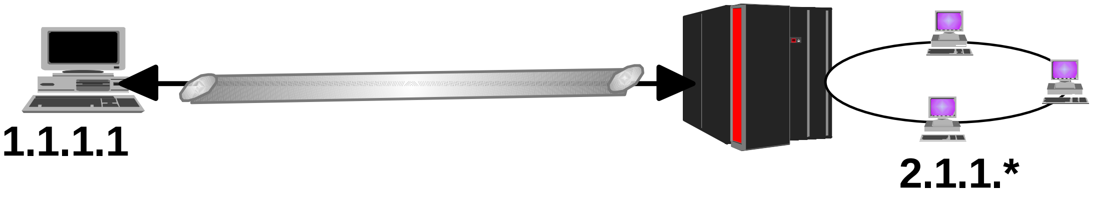
What about this encapsulation mode?

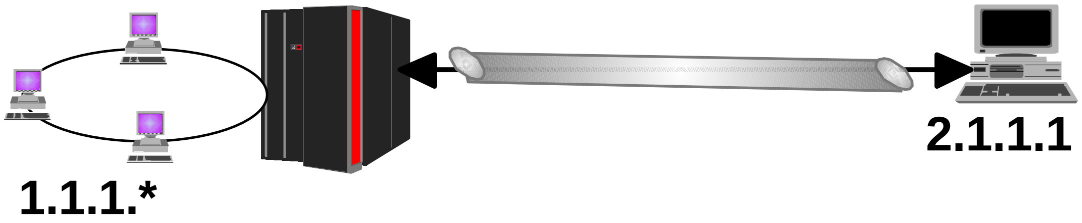
- Two options
  - Tunnel
  - Transport
- What's it for?
  - It tells IP how to construct the IPSec packet
- How do I decide?
  - If either of the tunnel endpoints is not a data endpoint
    - This means one or both tunnel endpoints are acting as a gateway
    - Tunnel mode must be selected
  - If both of the tunnel endpoints are also the data endpoints
    - This means both tunnel endpoints are acting as a host
    - Tunnel or transport may be selected
      - Usually transport mode is used in this case

Encapsulation mode (continued)

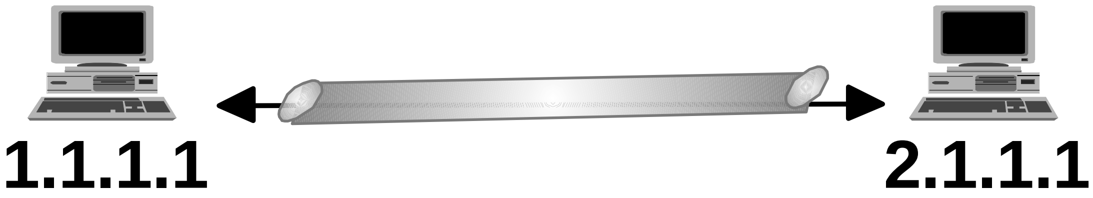
- □ Must use tunnel mode:







- □ May use tunnel or transport mode:



How do I want to perform key management?

□ Two options

- Manually
  - Managed by administrative procedures defined locally
  - Referred to as manual VPN on OS/390
- Dynamically
  - Managed by the Internet Key Exchange (IKE) protocol as defined by the IETF
  - Referred to as dynamic VPNs on OS/390

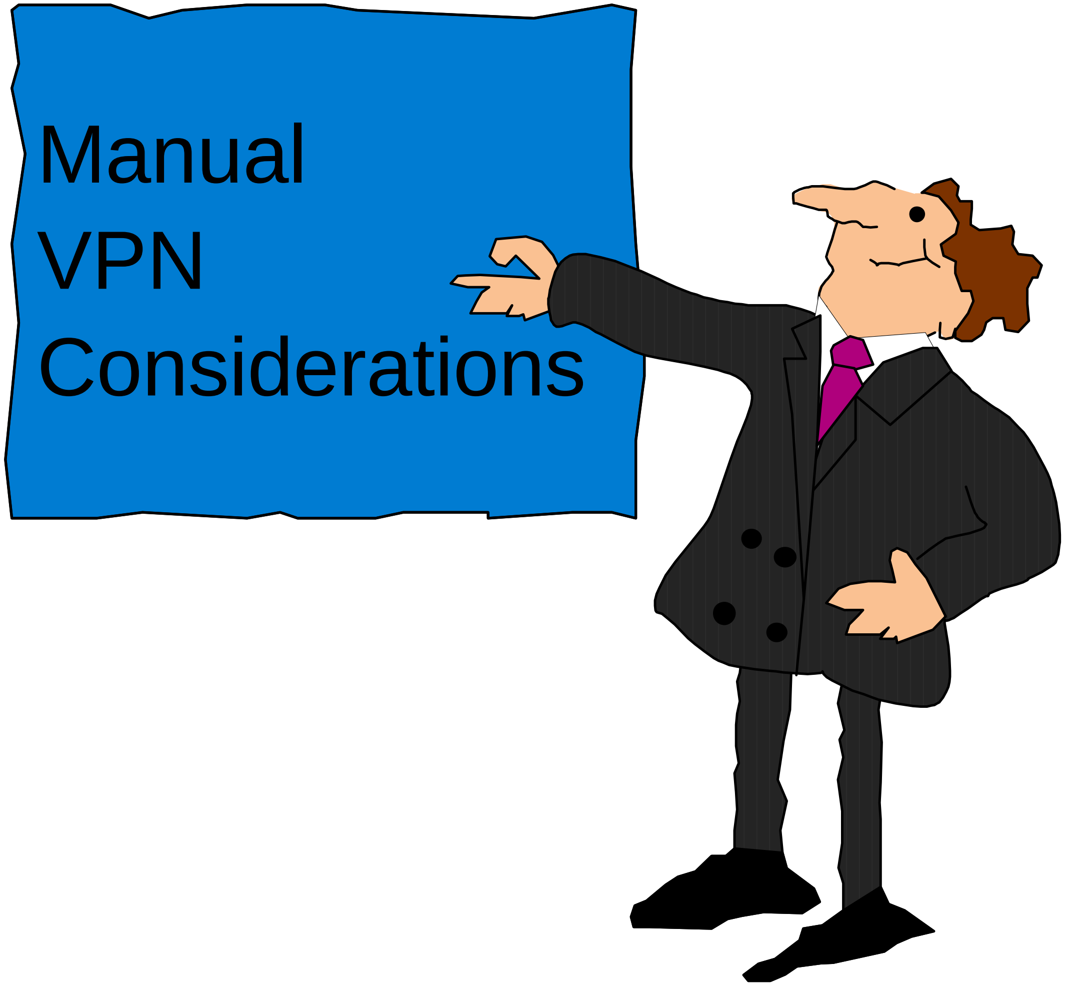
□ Over the long run dynamic VPNs are easier to manage than manual VPNs

□ Initially dynamic VPNs have a steeper learning curve than manual VPNs

How long do I want the VPN to last?

□ Applies to both Manual and Dynamic VPNs

- **In the manual case**
  - **Could be used to signal that a manual re-keying should take place**
- **In the dynamic case**
  - **Could be used to prevent run on negotiations**
    - **Some implementations will terminate a VPN after some period of inactivity**
      - ○ OS/390 does not



Manual VPN Considerations

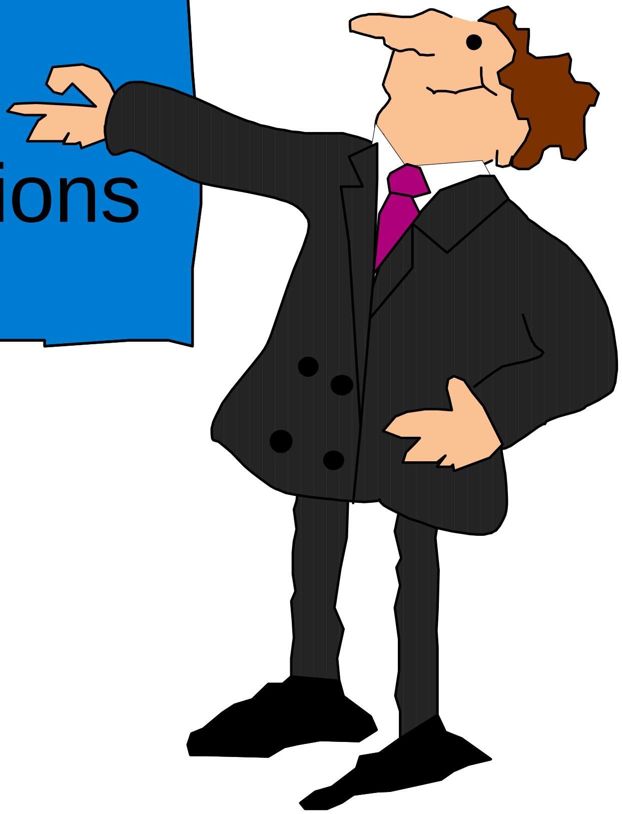
Manual VPN considerations

- □ Where do the cryptographic keys come from?
  - ● Mutual agreement between tunnel endpoint administrators
    - – Have keys automatically generated
      - ▸ Keys need to agree on both endpoints
      - ▸ Only one endpoint can automatically generate a key
    - – Enter their own keys
    - – Import/Export keys as part of a tunnel definition
      - ▸ Limited use if one of the endpoints is not as OS/390

- □ How do I exchange these keys?
  - ● You decide
    - – Sneaker net
    - – Secure e-mail
    - – US mail
    - – Phone

- □ How do I refresh these keys?
  - ● It's up to you
    - – Manual VPNs on OS/390 must be shutdown to refresh keys

Dynamic VPN Considerations

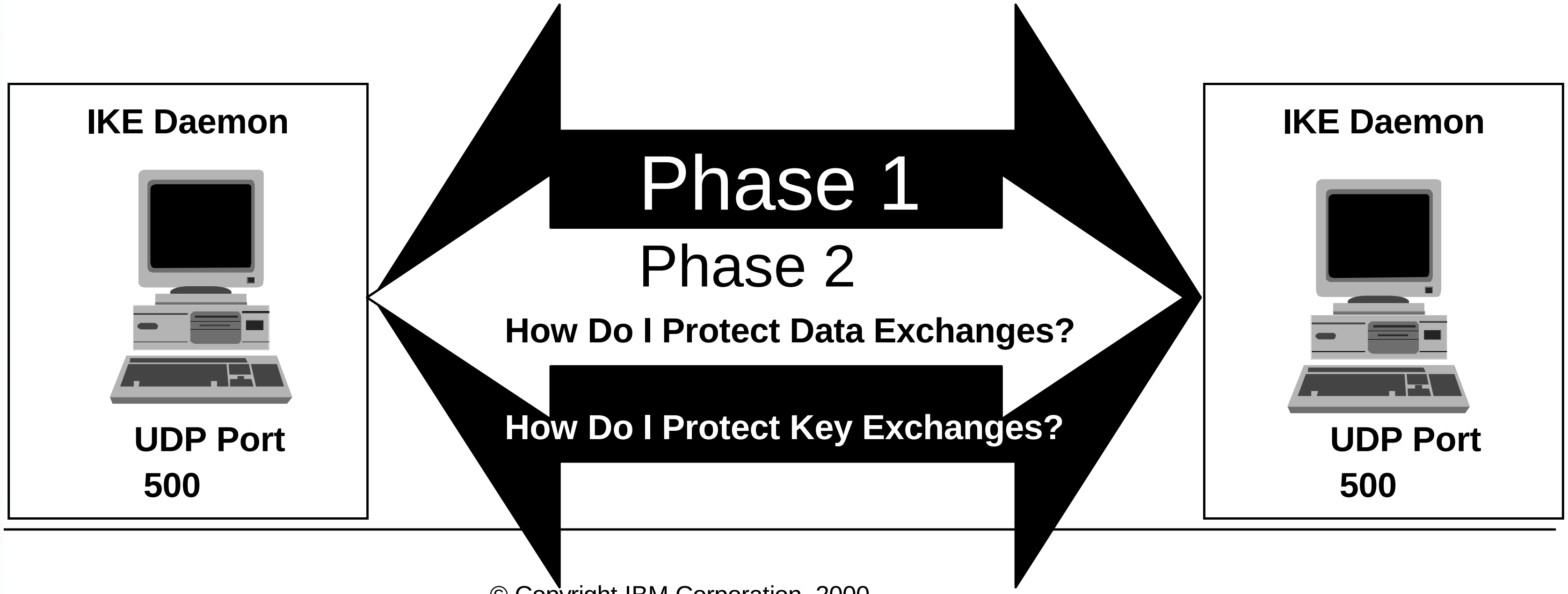


What is IKE?

- IKE is the Internet Key Exchange - RFC 2409
  - **Defined by the IETF IPSec working group**
  - **Related RFCs**
    - **RFC 2408 Internet Security Association and Key Exchange Protocol**
    - **RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP**
  - **Provides**
    - **Dynamic creation of cryptographic keys**
    - **Dynamic negotiation of how to protect data and key exchanges**
      - **Can also negotiate IP compression algorithms**
        - Not discussed in this presentation

What is IKE (continued)?

- Both tunnel endpoints must support IKE
  - IKE communicates using UDP port 500
- Uses a two phase approach
  - Phase 1
    - Decide how to protect key exchanges
    - Create keying material
  - Phase 2
    - Decide how to protect data in a VPN
    - Create cryptographic keys used to protect data in a VPN


IKE Daemon
UDP Port 500
Phase 1
Phase 2
How Do I Protect Data Exchanges?
How Do I Protect Key Exchanges?
IKE Daemon
UDP Port 500

How do I want to protect key exchanges?

□ What encryption algorithm do I want to use when exchanging keys?

- **DES_CBC_8 (Good)**
- **3DEC_CBC (Better)**

□ What hashing algorithm do I want to use?

- **MD5 (Good)**
- **SHA-1 (Better)**

□ What Diffie-Hellman Group do I want to use?

- **Group 1 (Good)**
- **Group 2 (Better)**

□ How often should I refresh the information I use to protect key exchanges?

- **Depends on encryption algorithm**
- **Can specify a time and a lifesize**

How do I know who I am talking to?

- □ IKE requires each tunnel endpoint to identify themselves
- □ What do I need to know?
  - ● **My identify**
  - ● **My peer's identify**
- □ What are examples of valid identities?
  - ● **IPV4 address**
    - – **1.1.1.1**
  - ● **Fully Qualified Domain Name**
    - – **endicott.ibm.com**
  - ● **RFC 822 Name (i.e. e-mail name)**
    - – **wierbows@us.ibm.com**
  - ● **X.500 Distinguished Name**
    - – **cn=Dave Wierbowski, ou=endicott, o=ibm,c=us**

How do I know my peer is who he says he is?

□ Two choices

- **Pre-shared key**
  - **Both sides agree on a arbitrary secret value called the pre-shared key**
    - ▸ **The pre-shared key is only used to authenticate, not protect**
  - **Need to answer:**
    - ▸ **What's our pre-shared key?**
- **RSA signature mode**
  - **Both side obtain a certificate**
    - ▸ **Each side uses their private key to create a signature**
    - ▸ **Each uses their peer's public key to verify their peer's signature**
    - ▸ **IBM IKE implementations obtain a peer's certificate as part of the IKE exchange**
  - **Need to answer:**
    - ▸ **What certificate authority do I need to obtain a certificate from?**
    - ▸ **What certificate authority do I want my peer to use?**
    - ▸ **Where are my certificates stored (i.e. where is my RACF keyring)?**

How do I want to protect data (revisited)?

- What's perfect forward secrecy (PFS)?
  - **The compromise of a key will only permit access to data encrypted with that key**
  - **Accomplished via a Diffie-Hellman Exchange**
- Additional IKE specific questions
  - **Do I want to use perfect forward secrecy when I generate keys to protect data in a VPN?**
    - **If yes, do want to use Diffie-Hellman group 1 or 2?**
  - **How often should I refresh the information I use to protect key exchanges?**
    - **Depends on encryption algorithm**
    - **Can specify a time and a lifesize**

Do I have the key and data policies I need?

- IKE manages
  - Keys
  - Security Associations
- IKE allows the algorithms dealing with key protection and data protection to be negotiated
- After deciding how I want to protect my key exchanges and data exchanges, I need ask:
  - Do I have an appropriate key policy and data policy defined?
    - If yes, then use it
    - If no, then create it
- IKE supports policies with multiple choices

Multiple options in a policy

□ Why would I allow multiple options?

- Because there may be more than one way to achieve my desired level of protection
- Examples:
  - I am only interested in data integrity and authentication
    - I could use the AH protocol
    - I could use the ESP protocol with NULL encryption
  - I want data to be sent encrypted, but I don't care how
    - I could use the ESP protocol with DES
    - I could use the ESP protocol with triple DES
  - I'm flexible
    - I might prefer to use triple DES to protect key exchanges, but tolerate DES if the keying material is refreshed every hour

Policy recommendations

- □ Start simple
  - ● Only offer one choice per policy
- □ Define a few simple policies and reuse them
- □ Examples:

	Gold Key Protection	Silver Key Protection	Bronze Key Protection
Encryption Algorithm	3DES_CBC	DES_CBC_8	DES_CBC_8
Hash Algorithm	SHA1	MD5	MD5
Authentication Mode	RSA Signature	RSA Signature	Pre-Shared Key
Diffie-Hellman Group	2	1	1
Lifetime	4 hours	4 hours	8 hours
Lifesize	10,000 KB	Infinite	Infinite

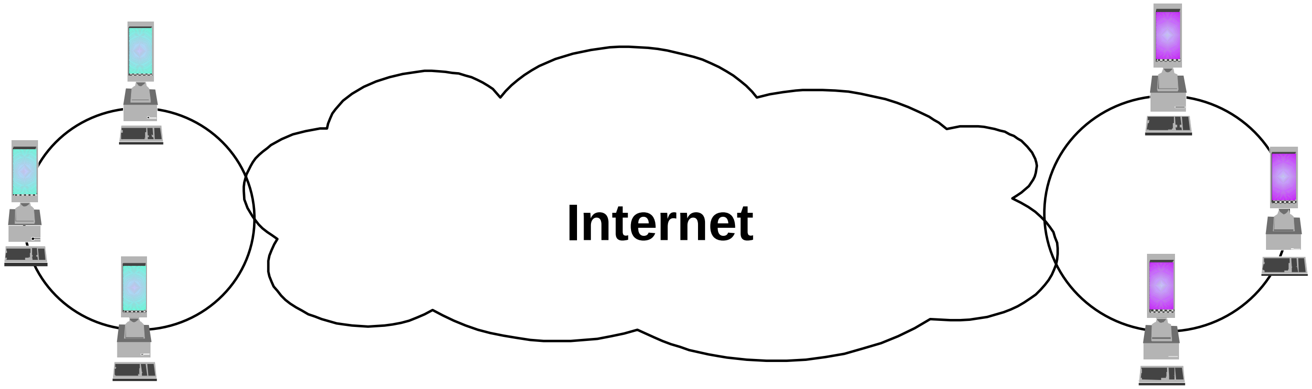
Policy recommendations (continued)

	Gold Data Protection	Silver Data Protection	Bronze Data Protection
Encryption Algorithm	3DES_CBC	DES_CBC_8	NULL
Authentication Algorithm	HMAC_SHA	HMAC_MD5	HMAC_SHA
PFS Group	2	1	None
Lifetime	1 hour	1 hours	2 hours
Lifesize	10,000 KB	10,000 KB	Infinite

Sample Walk-through:

Manual VPN

What do I want to protect?



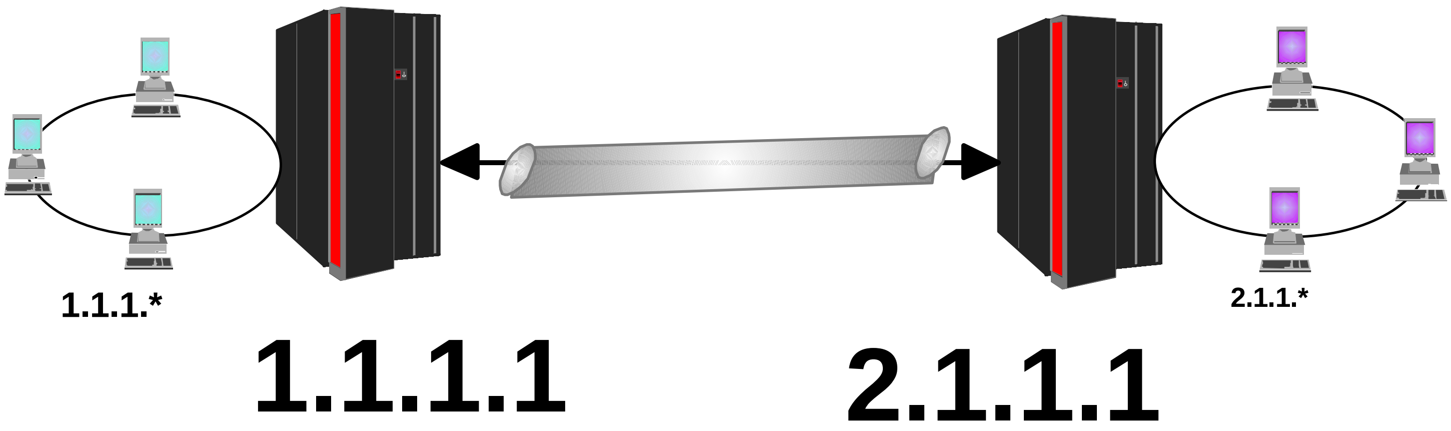
1.1.1.* **2.1.1.***

□ All traffic between subnet 1.1.1.* and 2.1.1.*

□ Where used:

- **On a filter rule**
  - **fwconns**
    - **Source network object**
    - **Destination network object**

Where do I want to protect?



- Between the firewall on subnet 1.1.1.* and the firewall on subnet 2.1.1.*
- Where used:
  - **fwtunnl - addr option**
  - **fwtunnl - remaddr option**

How do I want to protect data?

□ Do I need data privacy?

- **Yes**

□ Do I need data integrity and/or data origin authentication?

- **Yes**

□ I will use the ESP Protocol with the following options:

Based on RFC:	2406
Authentication Algorithm:	HMAC-SHA
Encryption Algorithm:	3DES_CBC
Encapsulation Mode:	Tunnel

□ Where used:

- **fwtunnl - policy option (encr) and possibly destpolicy options**
- **fwtunnl - newheader option**
- **fwtunnl - srcESPauth options and possibly destESPauth option**
- **fwtunnl - encrypthow options and possibly destencrypthow option**
- **fwtunnl - mode option**

How long do I want the VPN active?

- 480 minutes (8 hours)
- Where used:
  - fwtunnl - timeout option
    - 1 to 44640 minutes (31 days)
    - Infinite life

Cryptographic key considerations

□ Where do the cryptographic keys come from?

- **Have keys automatically generated**
- **Where done:**
  - **fwtunnl - srcESPencrkey option**
  - **fwtunnl - dest ESPencrkey option**
  - **fwtunnl - srcESPauthkey option**
  - **fwtunnl - destESPauthkey option**

□ How do I exchange these keys?

- **Secure e-mail**

□ How do I refresh these keys?

- **Secure e-mail every 8 hours**
- **Administrator reads new keys and updates tunnel definition**
- **Both sides need to refresh and activate simultaneously**

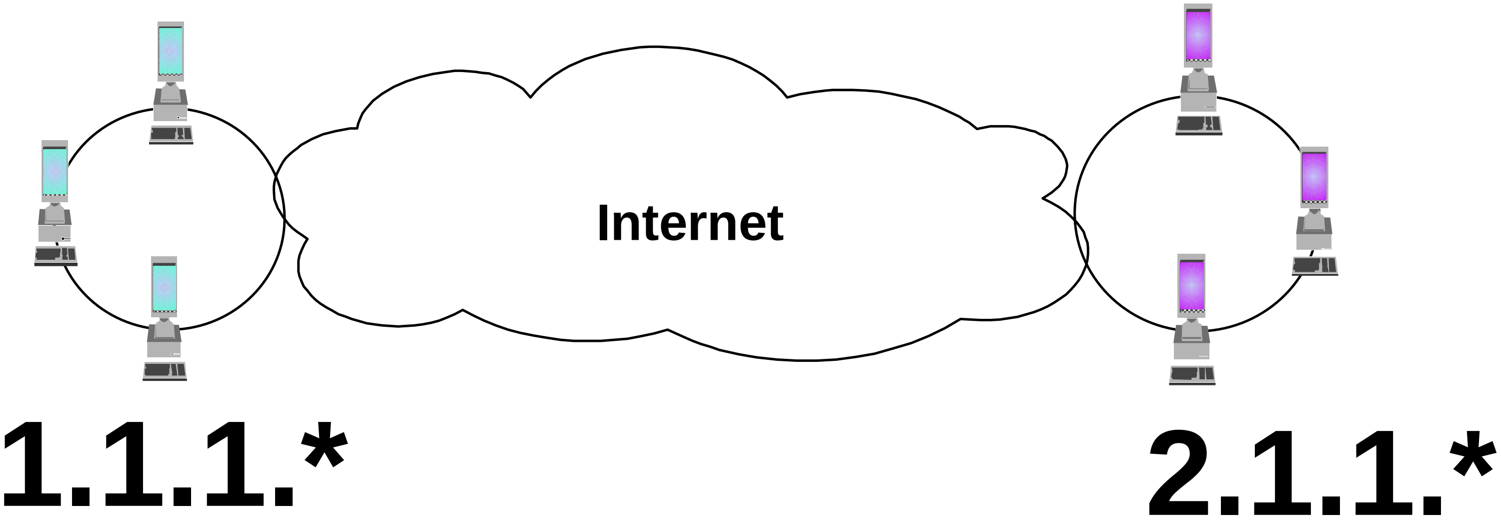
Items not covered by these questions

- Options on the fwtunnl command
  - **Tunnel IDs**
  - **SPIs**
  - **Replay protection**
  - **Autoactivate**
  - **AH attributes**
- How Tunnel IDs are related to filter rules
  - **fwservice - tunnel option**
  - **fwfrule - tunnel option**

Sample Walk-through:

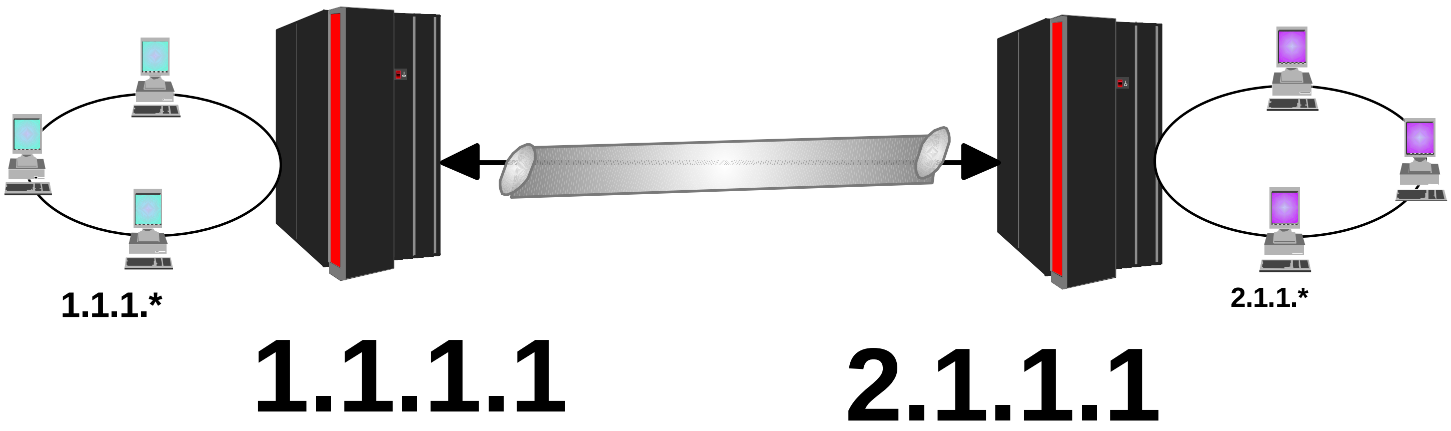
Dynamic VPN

What do I want to protect?



- All traffic between subnet 1.1.1.* and 2.1.1.*
- Where used:
  - On a filter rule
    - fwconns
      - Source network object
      - Destination network object

Where do I want to protect?



- ☐ Between the firewall on subnet 1.1.1.* and the firewall on subnet 2.1.1.*
- ☐ Where used:
  - ● fwkeysrv - ipaddr option
    - – **Two key server entries will be defined**
    - – **Depending on a number of factors, one or both entries may contain an IP address**

How do I want to protect data?

□ Do I need only data privacy?

- **Yes**

□ Do I need only data integrity and/or data origin authentication?

- **Yes**

□ I will use the ESP Protocol with the following options:

Based on RFC:	2406
Authentication Algorithm:	HMAC-SHA
Encryption Algorithm:	3DES_CBC
Encapsulation Mode:	Tunnel

□ Where used:

- **fwesptran - authalg option**
- **fwesptran - encralg option**
- **fwesptran - mode option**

How long do I want the VPN active?

- ~~480 minutes (8 hours)~~ 10080 (1 week)
  - I would allow a longer life with a dynamic VPN
    - Keys are refreshed automatically
      - Keys will be refreshed even if the dynamic VPN has been inactive (i.e. no traffic has been sent in it since the last refresh
- Where used:
  - fwdyntun - connlifetime option
    - 1 to 525600 minutes (1 year)
    - Infinite life

How do I want to protect key exchanges?

- □ What encryption algorithm do I want to use?
  - **3DEC_CBC (Better)**
  - **fwkeytran - encralg option**
- □ What hashing algorithm do I want to use?
  - **SHA-1 (Better)**
  - **fwkeytran - authmeth option**
- □ What Diffie-Hellman Group do I want to use?
  - **Group 2 (Better)**
  - **fwkeytran - dhgrp option**
- □ How often should I refresh the information I use to protect key exchanges?
  - **4 hours or 10,000 KB**
  - **fwkeytran - itime and isize options**
    - – **fwkeytran - rtime and rsize options**

How do I know who I'm talking to?

- □ What is my identity?
  - ● IPv4 address of 1.1.1.1
  - ● fwkeysrv - idtype and authid options
- □ What is my peer's identify
  - ● e-mail name of firewall@branch.mycompany.com
  - ● fwkeysrv - idtype and authid options
- □ Two key server entries will be defined

How do I know my peer is who he says he is?

- I'll pick RSA signature mode
  - What certificate authority do I need to obtain a certificate from?
    - My company's private CA with a subject alternate name of 1.1.1.1
      - If I don't have such a certificate I need to obtain it via RACF's RACDCERT command
  - What certificate authority do I want my peer to use?
    - My company's private CA
      - The certificate authority certificate must be on my keyring
      - fwcertauth - label option
      - fwauthinfo - certauth options
  - Where are my certificates stored (i.e. where is my RACF keyring)?
    - The RACF keyring named "mykeyring"
    - Owned by FWKERN
      - fwkeyring - keyring option
- If pre-shared key was picked
  - fwauthinfo shkey option
      - Entered as a hex string on OS/390
        - C1C2C3F1F2F3 (the EBCDIC string ABC123)
        - 616263313233 (the ASCII string ABC123)

How do I want to protect data (revisited)?

- Do I want to use perfect forward secrecy when I generate keys to protect data in a VPN?
  - **Yes, I'll use PFS Group 2**
  - **fwdatapol - pfs option**
- How often should I refresh the information I use to protect key exchanges?
  - **4 hours or 10,000 KB**
  - **fwesptran - itime and isize options**
    - **fwesptran - rtime and rsize options**

Do I have the key and data policies I need?

- Yes.
  - I'm using Gold Key Protection and Gold Data Protection
- Objects used to define new policies
  - Key
    - fwkeypol
    - fwkeyprop
    - fwkeytran
  - Data
    - fwdatapol
    - fwdataprop
    - fwesptran
    - fwahtran

Items not covered by these questions

- Where is key policy specified?
  - **fwkeysrvgrp**
    - **Binds a "local" fwkeysrv object and "remote" kwkeysrv objects with a key policy**
- Where is data policy specified?
  - **fwdyntun**
    - **Identifies information pertaining to the life cycle of a VPN**
      - **Connection lifetime**
      - **Who could create the VPN**
      - **What data policy should be used**
- How do dynamic tunnel policies related to filter rules?
  - **fwfrule - tunnel option**
    - **only valid for fwfrules with type of anchor**
- fwdynconns objects
  - **Identifies the remote tunnel endpoint and key policy to use for a particular data connection within a dynamic VPN**
  - **Only needed if the local system will activate the VPN**

OS/390 VPN Support by Release

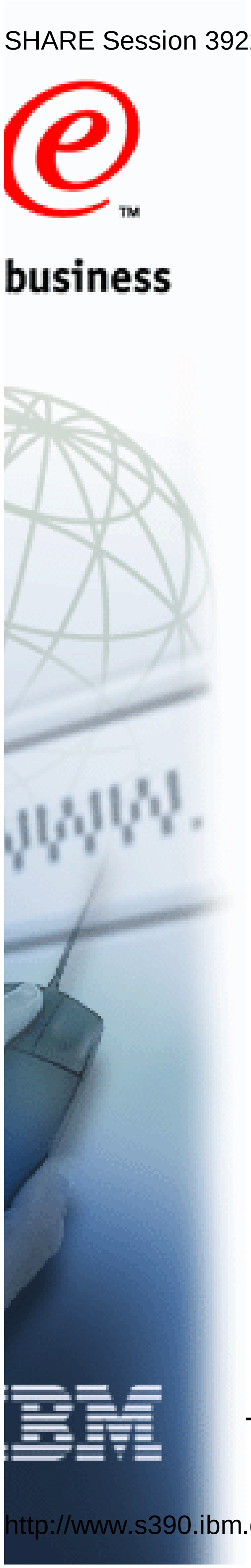
OS/390 VPN support by release

- R5
  - ● **Manual VPN Support**
    - **Support for RFCs 1825-1829**
    - **Tunnel mode only**
- **R6**
  - ● **Manual VPN Support**
    - **Add transport mode**
- **R7**
  - ● **Manual VPN Support**
    - **Add support for RFCs** 2401-2406 and 2410
- R8
  - ● Dynamic VPN Support
    - Support for RFCs 2407-2409

Where to Find More Information

□ The OS/390 Firewall Technologies Resource Web page

- **http://www.s390.ibm.com/products/mvs/firewall/resources.html**
- **See our OS/390 FIREWALL TECHNOLOGIES GUIDE AND REFERENCE**
  - **R4, R5, R6, R7, and R8 versions available**
    - ○ html format
    - ○ pdf format
- **See the following Freelance presentations:**
  - **OS/390 CONFIGURING VPNS ON OS/390**
  - **GETTING STARTED: IPSEC WITH CS FOR OS/390**
    - ○ Concentrates on actual configuration
  - **GETTING STARTED: IPSEC WITH CS FOR OS/390 (Boston)**
    - ○ Concentrates on gathering information for configuration
    - ○ This presentation
  - **FIREWALL OVERVIEW AND DIRECTIONS**
  - **GETTING STARTED USING THE FIREWALL**



Questions

???????