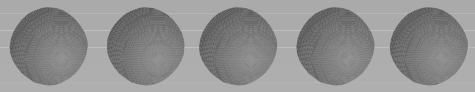
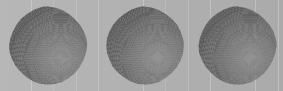


S 21

Directory-based Administration of Virtual Private Networks: Policy & Configuration



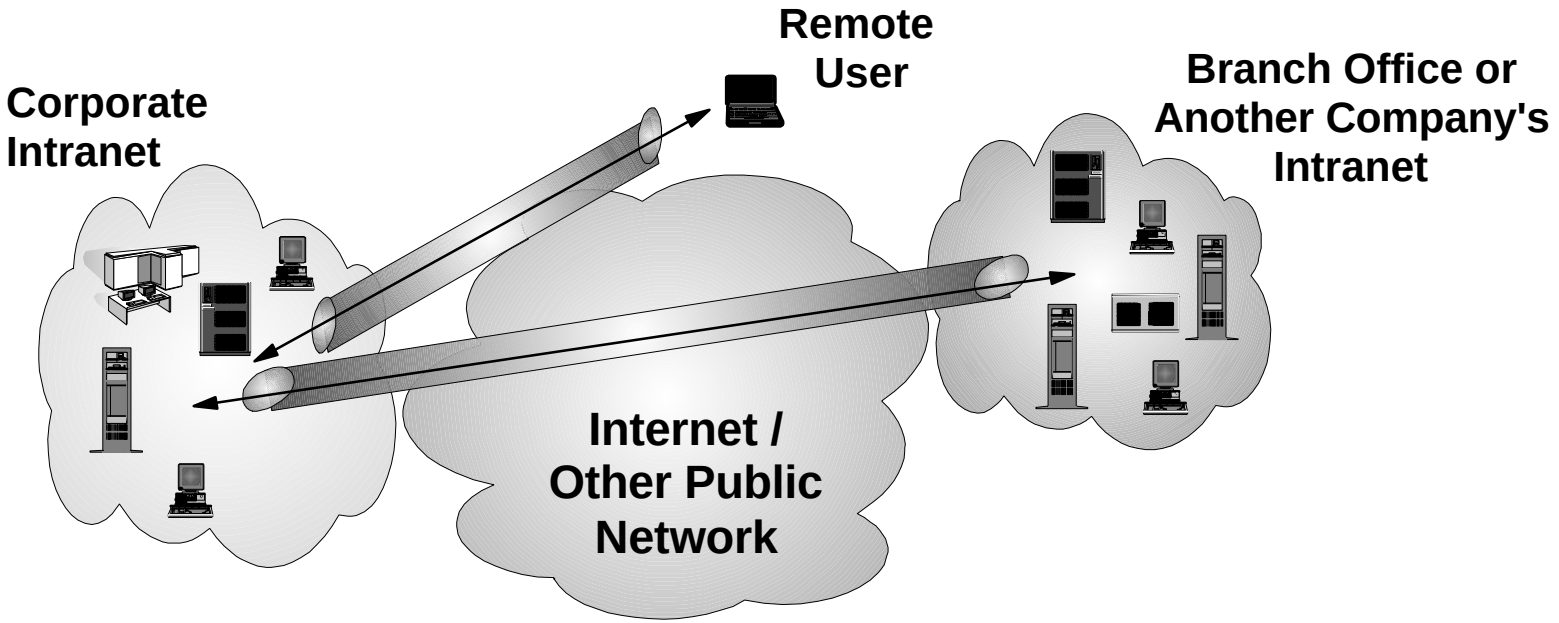
Charles A Kunzinger

kunzinge@us.ibm.com

Agenda

- What is a VPN?
- What is VPN Policy?
- "Box Configuration" & "Network Configuration"
- Schemas: Unambiguous descriptions
- Some examples
- Future Work

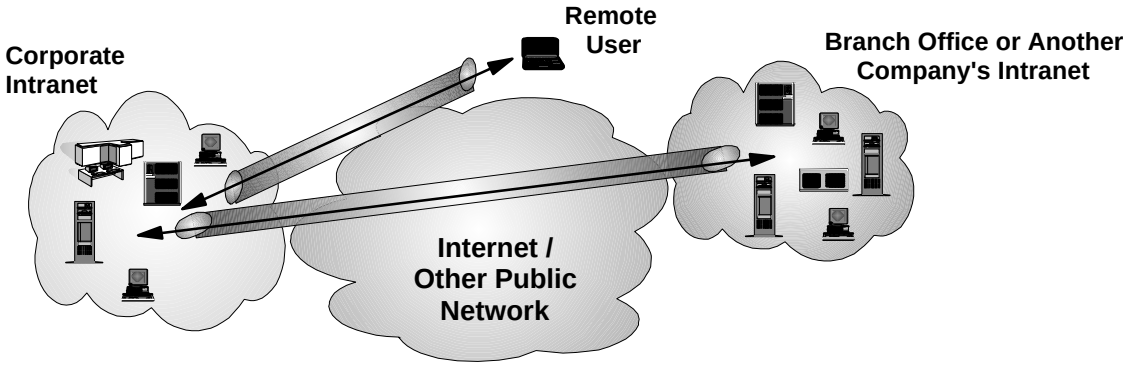
What is a VPN?



- A VPN (Virtual Private Network) is an extension of an enterprise's private intranet, across a public network (such as the Internet), creating a secure connection
  - *encrypt the user's datagrams*
  - *validate the user's datagrams*
  - *authenticate the source of the datagrams*
  - *establish & maintain cryptographic secrets*

e-business

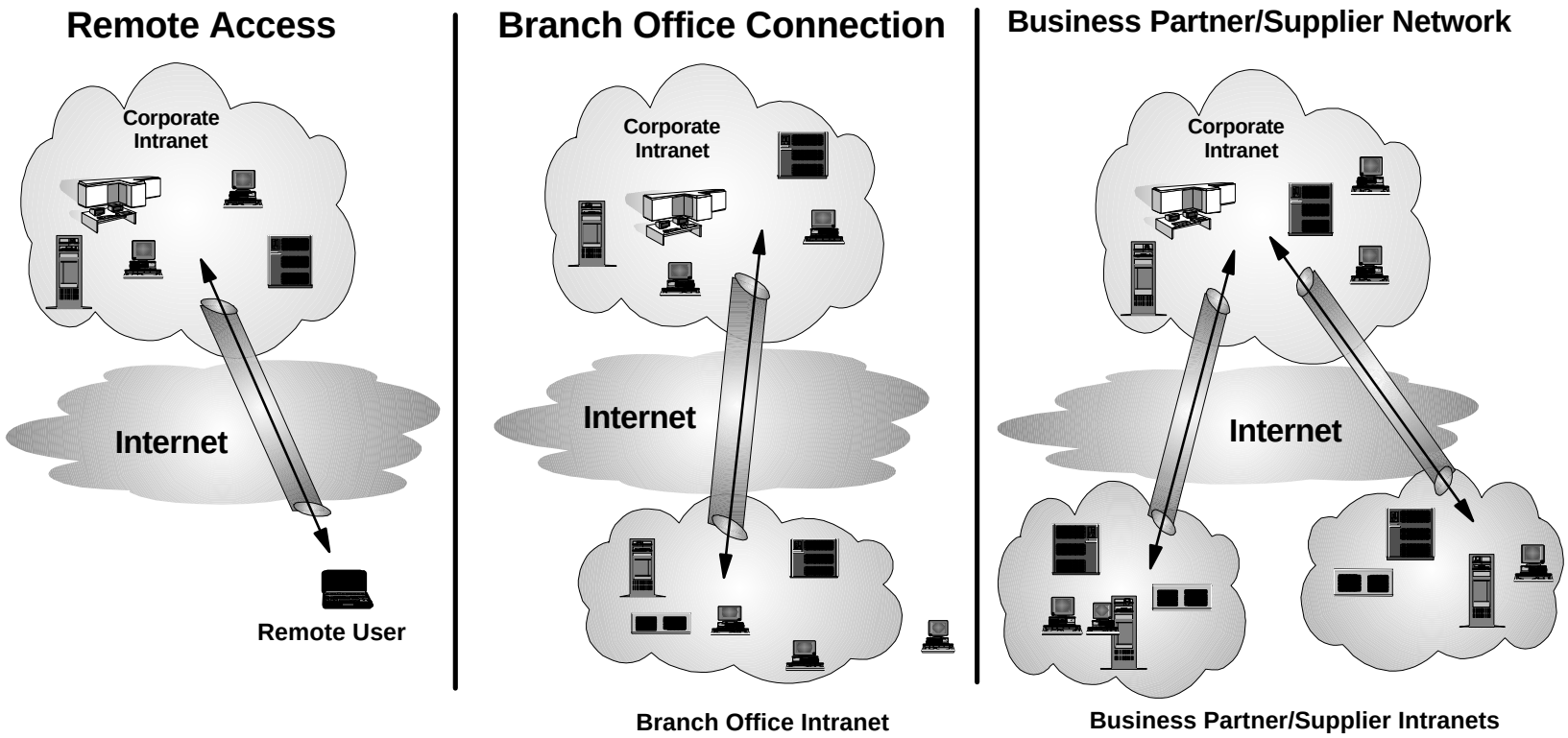
VPN Customer Value



- ► Easy, secure access to enterprise networks and resources:
  - Remote users and remote locations can access required information whenever they need to and from wherever they are
- ► Worldwide Access:
  - Internet access is available worldwide, where other forms of connectivity may be either not available or may be more expensive
- Cost Savings:
  - Cost effective access to the Internet via a local call to an ISP, versus expensive leased lines, long-distance calls and toll-free telephone numbers
  - Estimated 20%-47% savings in WAN costs and 60%-80% savings in remote access dial-up costs, per Infonetics Research, Inc

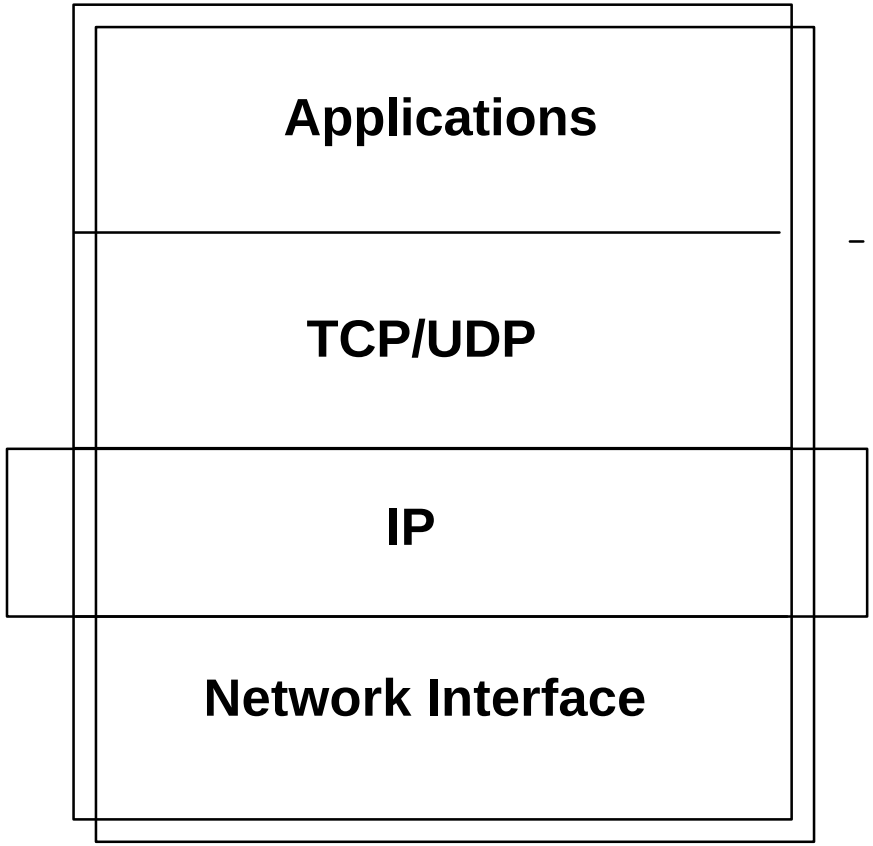
e-business

VPN Business Opportunities



- Remote Access Scenario
  - Problems: High administrative workload cost, expensive 800 or long distance costs
  - Solutions: VPNs exploit world-wide ISP reach and lower connectivity and administrative costs
- Branch Office Connection Scenario
  - Problems: Expensive Leased Line connections or part-time dial connections to home office
  - Solutions: VPNs provide 24-hour ease-of-use connectivity via inexpensive Internet links
- Business Partner/Supplier Network Scenario
  - Problems: Set-up/operational cost prohibitively high for smaller business partners; geographic limitations
  - Solutions: VPNs provide global, secure, cost-effective, end-to-end inter-company communication via Internet

Where Does IPSec Fit?



- S-MIME
- S-HTTP
- SET
- **IPSec (ISAKMP)**
- Others...

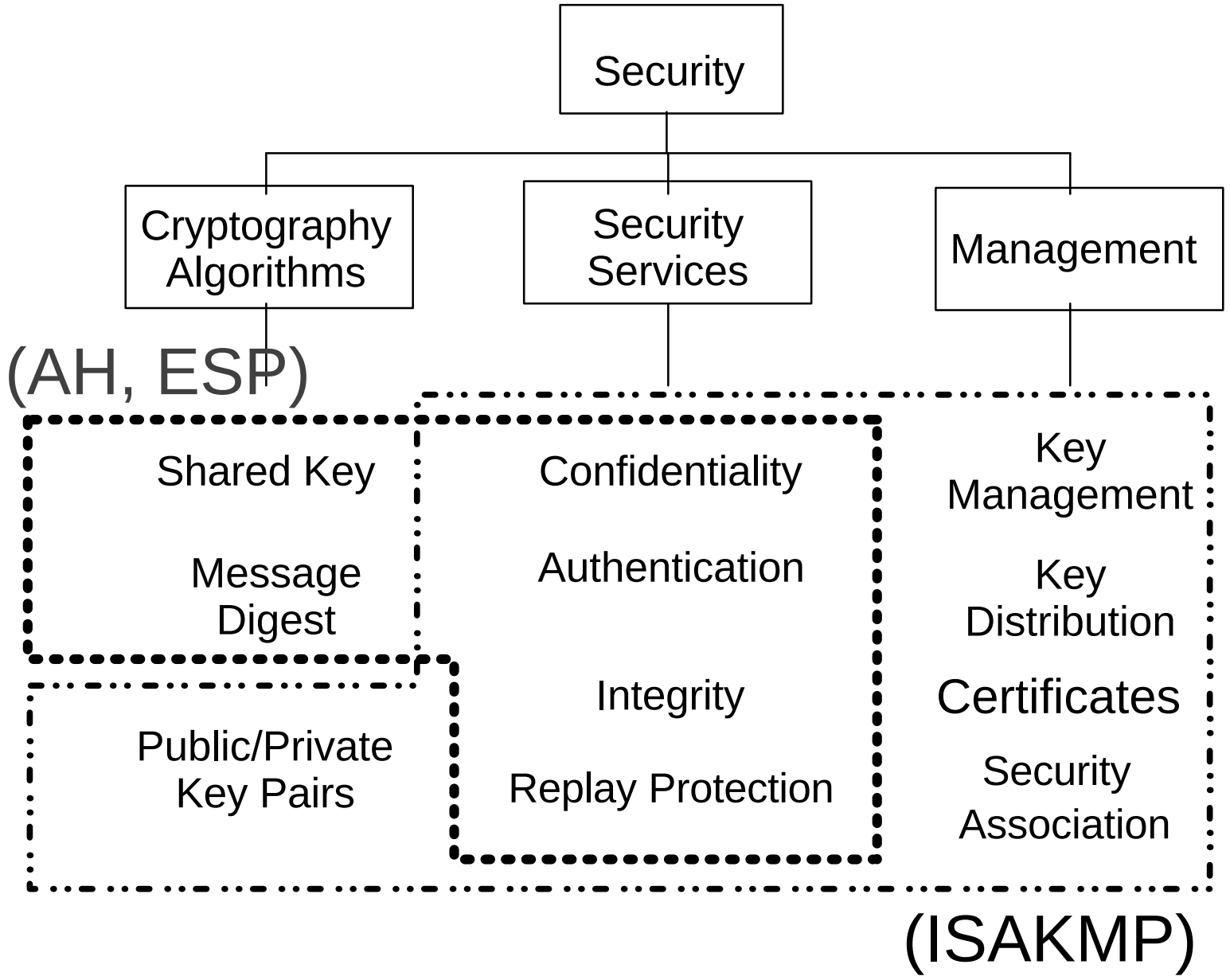
- SOCKS V5
- SSL
- TLS

- **IPSec (AH, ESP), packet filtering, tunneling**

- CHAP, PAP,MS-CHAP

- ***Network Layer (AH, ESP) protects user data***
- ***Application Layer (ISAKMP) manages security associations and securely generates and refreshes cryptographic keys***

Security Taxonomy



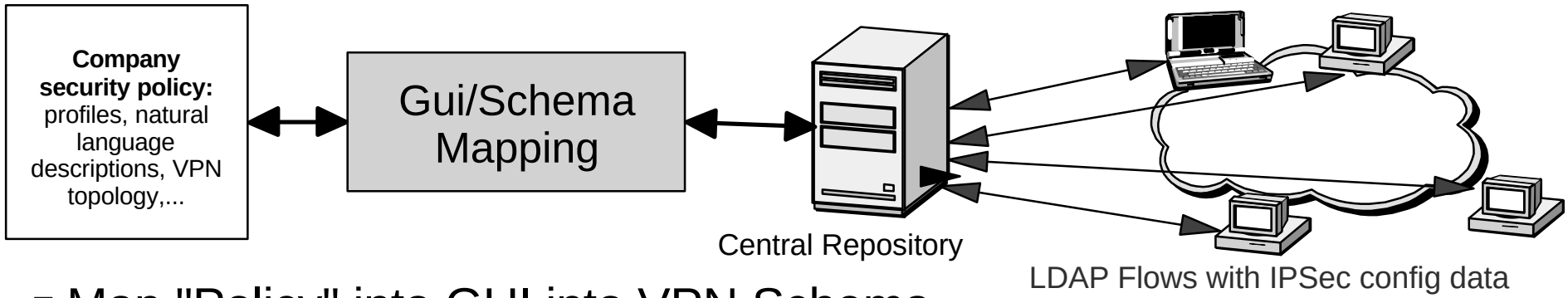
Policy Issues

- There are three:
  - ***What should it be:***
    - each company must analyze its own situation and set its own policy
  - ***Where it should be defined:***
    - per-box
    - centralized, network-centric
  - ***How it should be stored:***
    - LDAP Schema
    - Retrieval methods

Who sets VPN Policy?

- VPN's owner-operator sets the policy:
  - Membership
  - Access controls
  - Security details:
    - encryption requirements
    - authentication requirements
    - allowable protocols: http, ftp, telnet, ..., mail
- VPN's members (clients, servers, gateways) execute policy, but do not set it:
  - Centralized database with single point of control
  - Download box configurations, which carry out the VPN policy

VPN Policy



- Map "Policy" into GUI into VPN Schema
- Pre-defined profiles for typical configurations:
  - Branch Office Interconnect
  - Supplier Networks
  - Remote Access
- Centralized definition for all IPSec boxes in a given VPN
  - consistency checking
  - company-wide definition
- Database management:
  - individual boxes "pull in" their own configuration data
  - configuration data must be authenticated, but not necessarily kept confidential

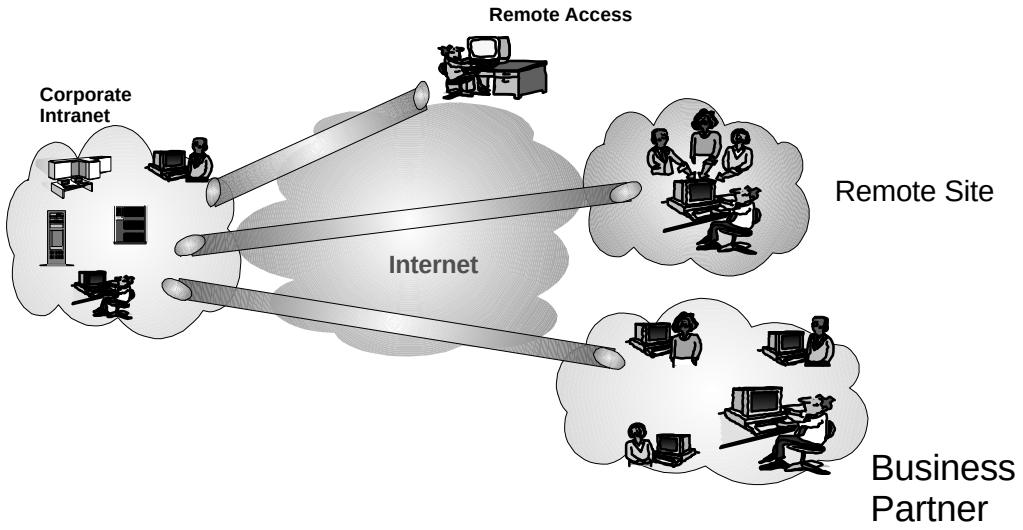
e-business

Box & Network Configuration

- Today most boxes are configured on an individual basis:
  - Firewalls guard your perimeter, regardless of what's done (or not done) at the far end of the communications path
- In today's VPN world, pairwise configuration of boxes is the norm:
  - same algorithms, shared keys, etc.
- In tomorrow's VPN world, network-wide configuration of boxes will be critical:
  - "Branch Office" is a mesh connection
  - "Business Partner" typically involves multiple enterprises
  - "Remote Users" may access their home networks or their business partners' networks
  - A given box may simultaneously participate in multiple scenarios

e-business

Box & Network Configuration...



- A given box may participate in multiple VPNs: e.g., Branch Office and Supplier Networks
- Each box (client, server, gateway) has its own Schema
- The collection of individual Schemas must implement a company's network-wide policy consistently

e-business

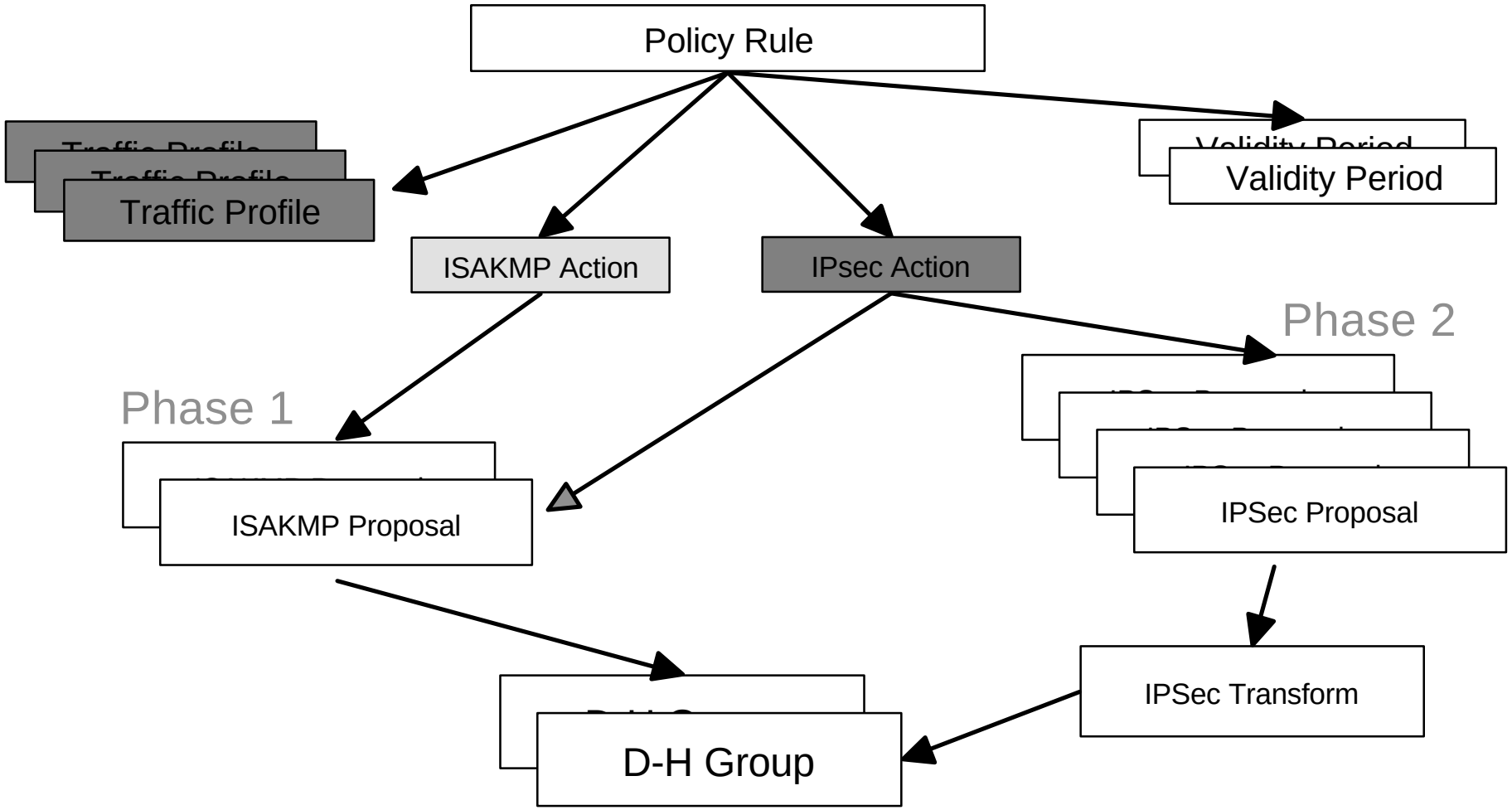
Policy, Parameters, & Schema

- ***Policy:*** describes what you want your VPN to do for you
- ***Parameters:*** detailed box-specific values that IPsec/IKE must instantiate
- ***Schema:*** formal mechanism to describe how IPSec and IKE configuration will be stored in the common database, for eventual retrieval via LDAP mechanisms

IPSec Schema

- Vocabulary is largely "IPsec-specific":
  - precise technical meanings
  - could be daunting to "non-experts"
- Standardized, open description of the configuration of a single VPN-capable box
- Two types of objects are described:
  - Generic: can apply to many Security Associations; reusable; unambiguous depiction of corporate VPN policy
  - Traffic-specific: define the end points between which a given SA can be instantiated; link topology to abstract policy

VPN Schema Overview



Legend:

Independent of end points

End point specific

e-business

Schema Model

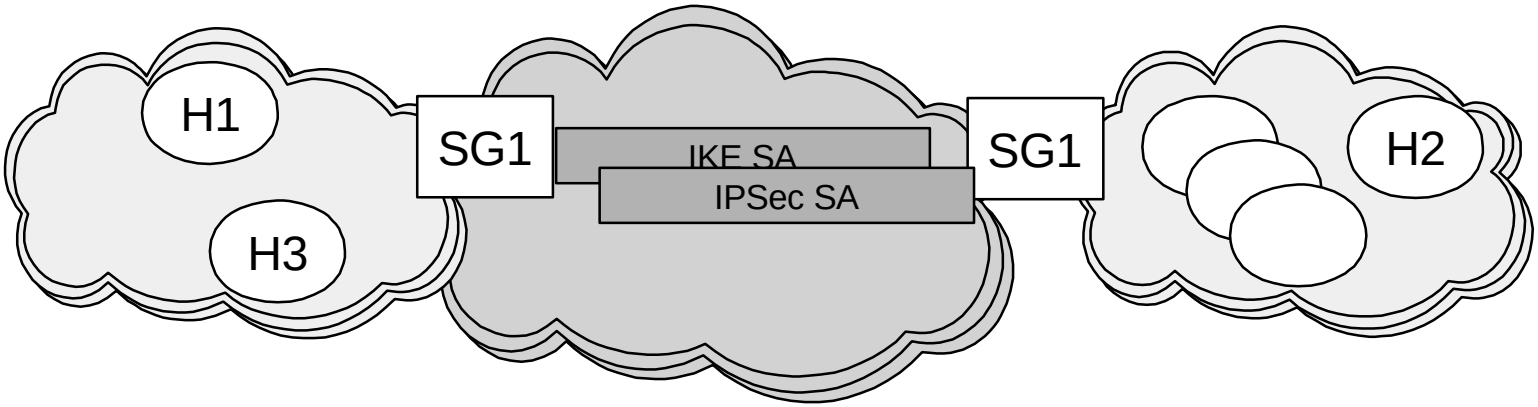
- If (conditions met) then (take indicated action)
- Conditions:
  - Traffic Profile: source & destination addresses, ports, interfaces, protocols, ID
  - Validity Period
  - IPSec Action: proxies' addresses, ports, protocols
- Actions:
  - ISAKMP Action
  - IPSec Action

Schema Classes...

- A single **Policy Rule** can point to:
  - multiple **Traffic Profiles**
  - multiple **Validity Periods**
  - single **ISAKMP Action**
  - single **IPSec Action**
- **ISAKMP Action**: Phase 1 exchange mode, lifetimes, public key (certificate) information, pointer to "ISAKMP Proposals"
- **ISAKMP Proposal**: algorithms & authentication methods, lifetimes, D-H group. (*multiple per "ISAKMP Action"*)
- **IPsec Action**: *proxy info*, *tunnel end point*, lifetimes, pointer to protection suites, pointer to a coupled "ISAKMP Proposal".
- **IPSec Transforms**: algorithm details, lifetimes, D-H group. (*multiple per "IPSecAction"*)
- **D-H Group**: general D-H group characteristics; pointed to by "IPSec Proposals" and "ISAKMP Proposals
- There ae some "non-standards" items in the Schema:
  - ISAKMP Connection
  - "Lifetime" for ISAKMP Connection as well as for ISAKMP SA
  - Override values for Lifetimes

e-business

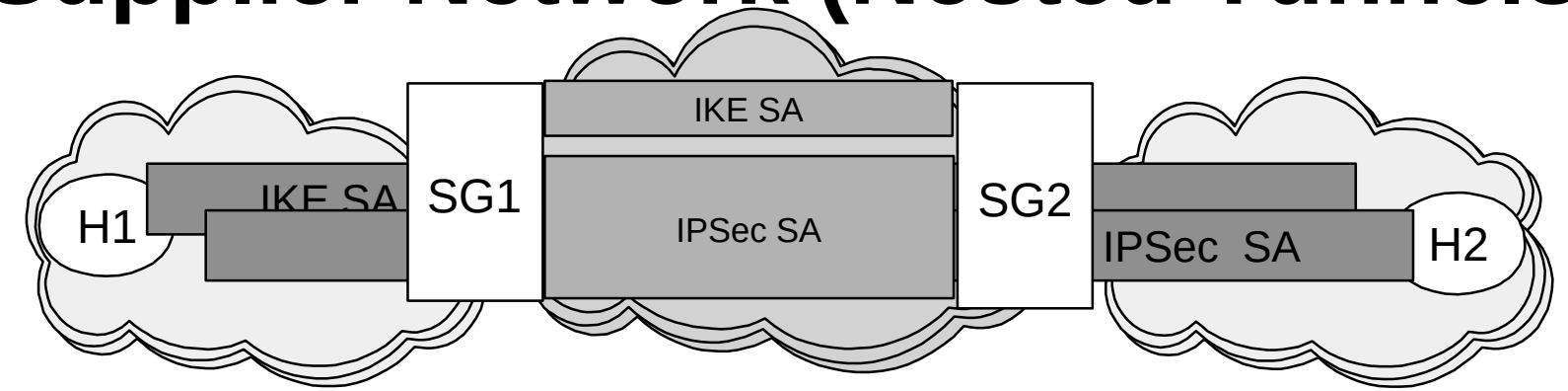
Branch Office Scenario



- Only SG1 and SG2 have VPN Schemas
  - Phase 1 SA terminates at SG1 & SG2
  - Phase 2 SA(s) terminate at SG1 and SG2
- If a multiple host pairs levy the same special requirements on the Gateways, then appropriate "proxy info" must be included in the **IPSec Action** defined in both SG1's and SG2's schema
- If multiple host pairs levy different special requirements on the Gateways, then multiple Policy Rules must be created

e-business

Supplier Network (Nested Tunnels)



- Independent IKE negotiations:
  - SG1 & SG2 have a set of SAs between them
  - H1 and H2 have a set of SAs between them
  - H1-H2 SAs are nested inside SG1-SG2 IPSec SA
- SG1-SG2 IPSec SA(s) must include "proxy info" on intranet end points:
  - each "proxy pair" needs a different SG1-SG2 IPSec SA
  - each different IPSec SA implies a separate **IPSec Action**
  - each **IPSec Action** implies a distinct Policy Rule...
  - ...and so on as we get into even more complex examples

e-business

Box Configuration Implications...

- A VPN Schema alone is not sufficient to guarantee network-wide consistent policy:
  - It guarantees unambiguous "per-box" descriptions of IPSec characteristics
  - It does not guarantee acceptable end-to-end results

- In previous two examples, a network topology diagram was needed to visualize the correct "schema" to construct
- If boxes are configured individually, then each administrator must work off the same topology diagram, including the specific IP address & port information
- Boxes that participate in all three IBM scenarios (Branch Office, Supplier, Remote Access) will be especially difficult to configure accurately

e-business

Policy Questions...

- Mechanisms for a box to retrieve its own configuration information from Directory?
- Mechanisms for checking consistency across a large set of individually configured boxes?
  - outright misconfiguration errors (e.g., does each rule have a "mirror image"?)
  - overlapping policy rules (what breaks the ties?)
- Consistency of terminology between GUI panels and LDAP Schema?
- Mapping of GUI entries into the Schema formats?

IBM VPN Policy Groundrules

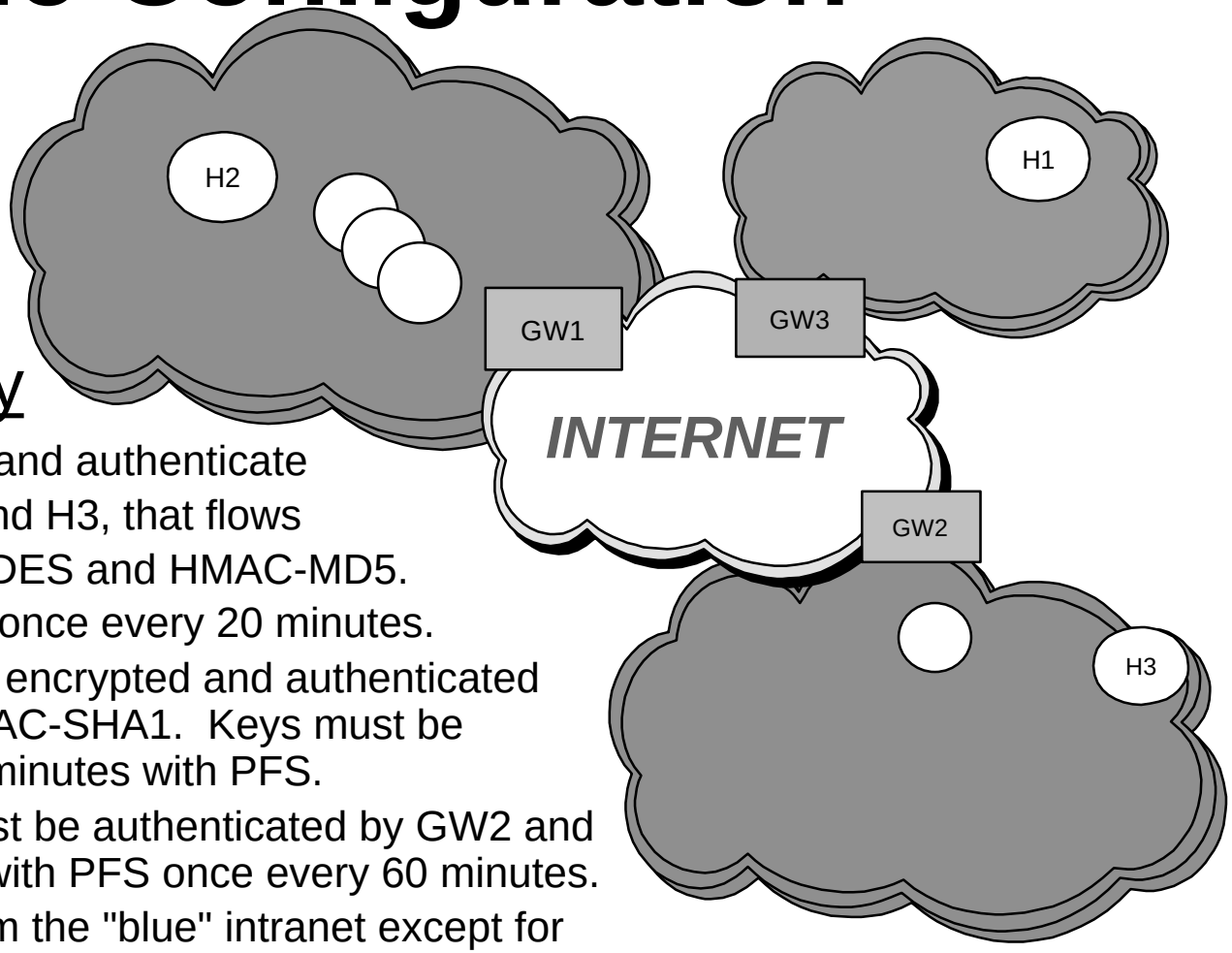
- Since "Schema" is to be an open standard, it takes precedence over GUIs
- IBM GUIs must demonstrate one-to-one mapping onto the VPN Schema
  - All profiles possible that can be configured with a GUI must map into a matching Schema
  - GUIs need not support all profiles that are possible under VPN Schema
- GUI terminology must be common across all IBM VPN products, but can use more"colloquial" terms than the Schema

e-business

Sanity Check...

- Define a benchmark "complex VPN configuration" involving:
  - clients, servers, firewalls, and routers
  - elements from all scenarios: branch office, supplier, remote access
- Demonstrate "per box" configuration using GUI
- Produce composite LDAP VPN Schema
- Learn from our mistakes...

Sample Configuration



Example VPN Policy

1. GW1 and GW2 must encrypt and authenticate from all hosts, except from H2 and H3, that flows between GW1 and GW2, using DES and HMAC-MD5. Keys must be refreshed at least once every 20 minutes.
2. Traffic from H1 to H2 must be encrypted and authenticated end-to-end using 3DES and HMAC-SHA1. Keys must be refreshed at least once very 10 minutes with PFS.
3. Traffic between H2 nd H3 must be authenticated by GW2 and GW1. Keys must be refreshed with PFS once every 60 minutes.
4. GW1 must reject all traffic from the "blue" intranet except for packets from H1. And GW1 and GW3 must authenticate trafic flowing between themselves.
5. GW2 must reject all traffic to or from the "non-yellow" intranets.

e-business

Future Work

- LDAP-based "VPN Schema" accepted by IETF by 1Q'99 (industry-wide goal)
- IBM "Value-Adds" for VPNs:
  - Develop user-friendly front-end network configuration tool--"point & click" will:
    - Apply named policy elements between specific VPN-enabled boxes
    - Automatically generate corresponding VPN schema and load into central database
  - Develop automated consistency checker for VPN Policy across large numbers of boxes

e-business