Linux 2.6 CryptoAPI IPSec & FileSystems

Matthew G. Marsh

President, Paktronix Systems LLC

Chief Scientist, NEbraskaCERT

Overview

- Linux 2.6 Kernel CryptoAPI
  - What is it
  - Why is it
  - Who cares
- File System Support
  - CryptoLoop / DM-Crypt
  - NFSv4
- IPSec
  - Common Concepts
  - Mini-HowTo
- Examples & Discussion

Linux 2.6 CryptoAPI

- **What is it**
  - **Scatterlist Cryptographic API**
    - **Page vector arguments are directly operated upon**
    - **Designed to apply to paged SKB without linearization**
      - **Speed and generality are the result**
  - **API Layering (Highest to Lowest level)**
    - **Transform API (User Interface)**
    - **Transform Operations**
    - **Algorithm API**
  - **Currently three (3) main transform types**
    - **Cipher**
    - **Digest**
    - **Compression**

Linux 2.6 CryptoAPI

- Why is it
  - Main initial design goal was IPSec support
    - Due to political problems there was no kernel IPSec
    - Alexey Kuznetsov and Dave Miller got fed up
    - James Morris of NetFilter submitted a FrameWork
    - Code from KAME (USAGI) and ANK's NetLink
  - Consideration of the Kerneli CryptoAPI
    - Led to a broader modular design
    - Work on NAPI & Network API led to generalization
    - Concept of "All data is a Page"
  - Kernel Level allowed for Flexibility & Security
    - Dovetails nicely with the Linux Security Modules

Linux 2.6 CryptoAPI

- **Who Cares**
  - **Anyone involved in Securing Linux**
    - **Provides a modular infrastructure**
    - **API allows for unique & customized configurations**
    - **Extensible & Available at Boot Time**
    - **Files and FileSystems may be layered**
  - **Anyone involved in Network Linux**
    - **Any traditional transport may be encapsulated**
    - **Both Point and Network operations available**
    - **Differentiation down to the Port & Policy Level**
  - **You**
  - **Me**

File System Support

- CryptoLoop
  - Builds on original implementation under Kerneli
  - Concept of inserting crypto into Loop mount
    - All transactions through loop device intercepted
    - Ease of use
  - First available in 2.6 without patching - BUT -
  - Is scheduled for Deprecation in 2.6
  - Can use a file or a partition
    - File provides portability (CD/DVD - USB Storage)
    - Partition is best for Server Shares
  - Independent of Use (NFS/SAMBA/MARS)

File System Support

- **CryptoLoop - Continued**
  - **Requires Patched Utilities**
    - **CarryOver from previous Kerneli implementation**
    - **Patches are incompatible**
      - **Between other methods (Loop-AES, etc)**
      - **In some cases between utility and kernel releases**
  - **Key Management is Manual**
  - **Incompatible with Kerneli CryptoAPI**

File System Support

- **DM-Crypt - Device Mapper Crypto Target**
  - **Device Mapper - K2.6 Virtualized Block Devices**
    - **Used by LVM2 et al**
  - **Provides transparent virtual block encryption**
  - **Uses 2.6 CryptoAPI and device subsystem**
  - **Backward compatible with CryptoLoop mode**
  - **Flexible specification**
    - **IVgen (Initial Vector Generation)**
    - **Key**
    - **Symmetric Cipher**
  - **Kernel >= 2.6.4**
  - **Requires special device mapper tool (DMSetup)**
  - **After using dmsetup you can use normal utils**

File System Support

- **DM-Crypt - continued**
  - **Requires special tool (DMSetup)**
  - **After using dmsetup you can use normal utils**
  - **Example:**

```
# Get the number of blocks in your partition IE:  blockdev --getsize /dev/sdb1  returns 1333216
# Create the Hash key from a SALT and passphrase (IE; PakSecured Rulez!)
hashalot -s SALTY -x sha512 | cut -c 1-32
# Use the 32 bits spewed out above to create the crypto device
echo 0 1333216 crypt aes-plain {insert 32 hex from above} 0 /dev/sdb1 0 | dmsetup create datacrypt
# The first time you run this you will want to create the filesystem - remmed out here as we have already done this
# mke2fs -j /dev/mapper/datacrypt
# Now mount the filesystem
Mount /dev/mapper/datacrypt /mnt/crypto
# And use as normal - Note that when the filesystem is unmounted you can run dmsetup remove datacrypt to
# remove the device thus rendering the partition unreadable until the device is recreated
```

File System Support

- **DM-Crypt - continued**
  - **Filesystem encryption is Transparent**
    - **You can even share the system using MARS or SAMBA**
    - **Of course the shared data is not encrypted**
  - **Device is unmounted and removed = No READ!**
  - **The same sequence used above for partitions is equally valid for Files**
  - **Files can be shared in the encrypted state**
    - **CD/DVD/MARS/SAMBA**
    - **Mount the file using the appropriate commands…**
    - **All data transfers are encrypted**

File System Support

- NFSv4
  - Often mentioned as obviating DM-Crypt et al
    - Actually Orthogonal and complementary
  - Updates NFS protocol to provide CIA
  - Build on RPCSEC_GSS work
  - Adds Client/Server Security Negotiation
    - Provides for enforcement of Security Policy
    - Can require security schema support bi-directionally
  - Designed for future transparent extensions
  - Excellent in combination with IPSec transport

IPSec

- **Common Concepts**
  - **IP Security - Start with RFC 2401**

    IPsec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols

  - **This quote from RFC 2401 should be sufficient**
  - **IPSec provides methods to:**
    - **Select required security protocols**
    - **Determine algorithm(s) to use for selections**
    - **Put in place the necessary cryptographic keys**

IPSec

- **Common Concepts - continued**

  MYTH: Traditional IPSec is DES and MD5

  FACT: There are NO algorithm requirements

  - **Two Main Network parts of IPSec:**
    - **AH - Authenticating Header**
    - **ESP - Encapsulating Security Payload**
  - **Main Concept of IPSec security**
    - **SA - Security Association**
      - **SPI - Security Parameter Index**
      - **IP Destination Address**
      - **Security Protocol (AH or ESP) ID**
    - **Note Directionality is implicit**

IPSec

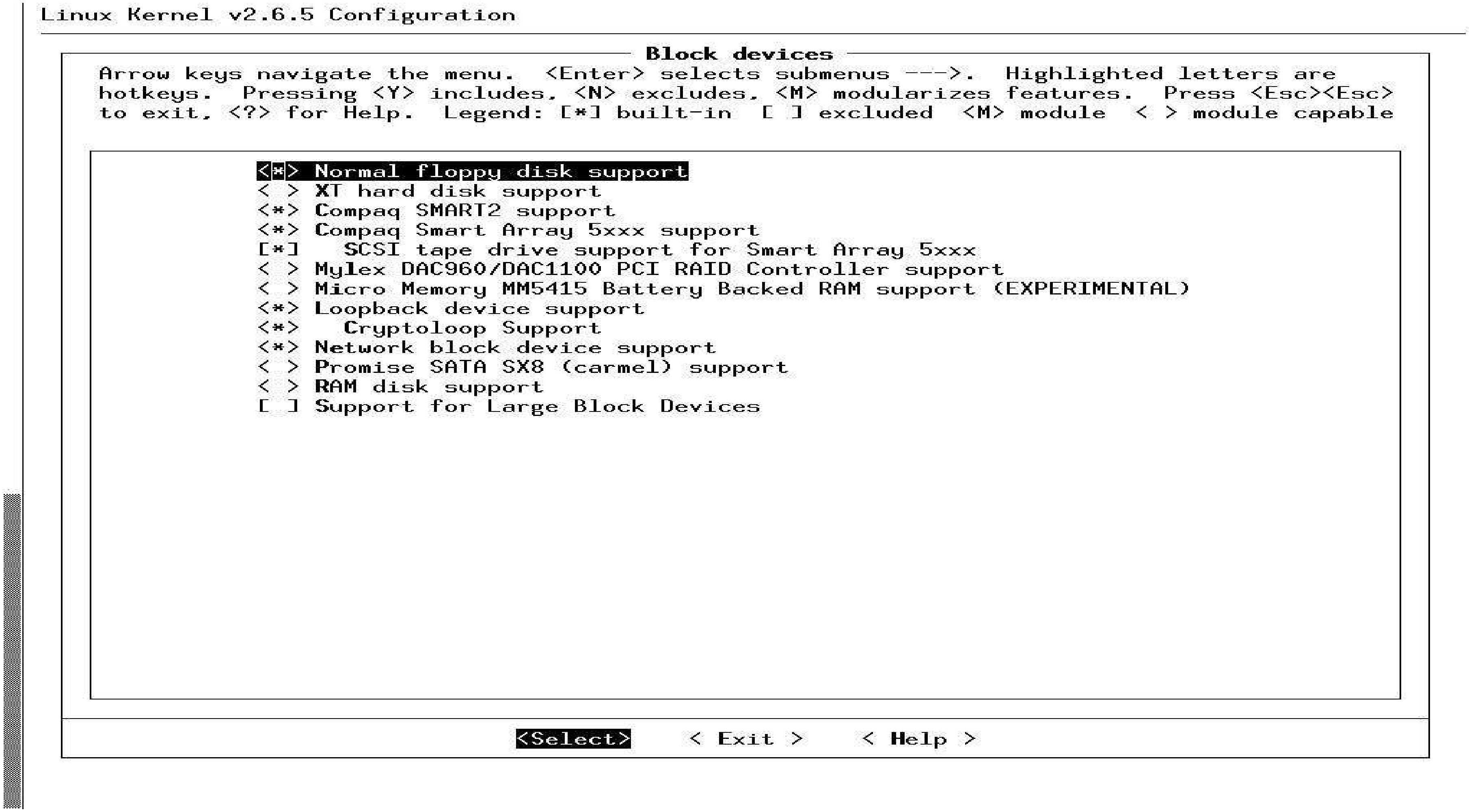
- **Common Concepts - continued**
  - **Biggest problem is the KEY problem**
    - **Symmetric cipher key exchange**
    - **How do you do it**
      - **SneakerNET**
      - **Decanting 32+ hex characters over the telephone!**
  - **IKE - Internet Key Exchange**
    - **ISAKMP**
      - **Internet Security Association & Key Management Protocol**
    - **Defines a two phase system of negotiation**
      - **Phase One uses PSK (PreShared Keys) or x509 certs**
        - **Sets up a ISAKMP SA**
      - **Phase Two sets up the actual connection SA(s)**

IPSec - Linux 2.6 Config

- **Kernel 2.6.5 is used for illustration**
  - 2.6.0+ is fine
- **Need ipsec-tools**
  - http://ipsec-tools.sourceforge.net
  - 0.3.1 is used in this session
- **Need IPRoute2 utility**
  - ONLY USE
    iproute2-2.4.7-now-ss020116-try.tar.gz
  - http://www.linuxgrill.com
- **Your system should be Linux 2.6 compliant**
  - PakSecured 2.4.18 is sufficient
  - PakSecured 2.6.4 is best

IPSec - Linux 2.6 Config

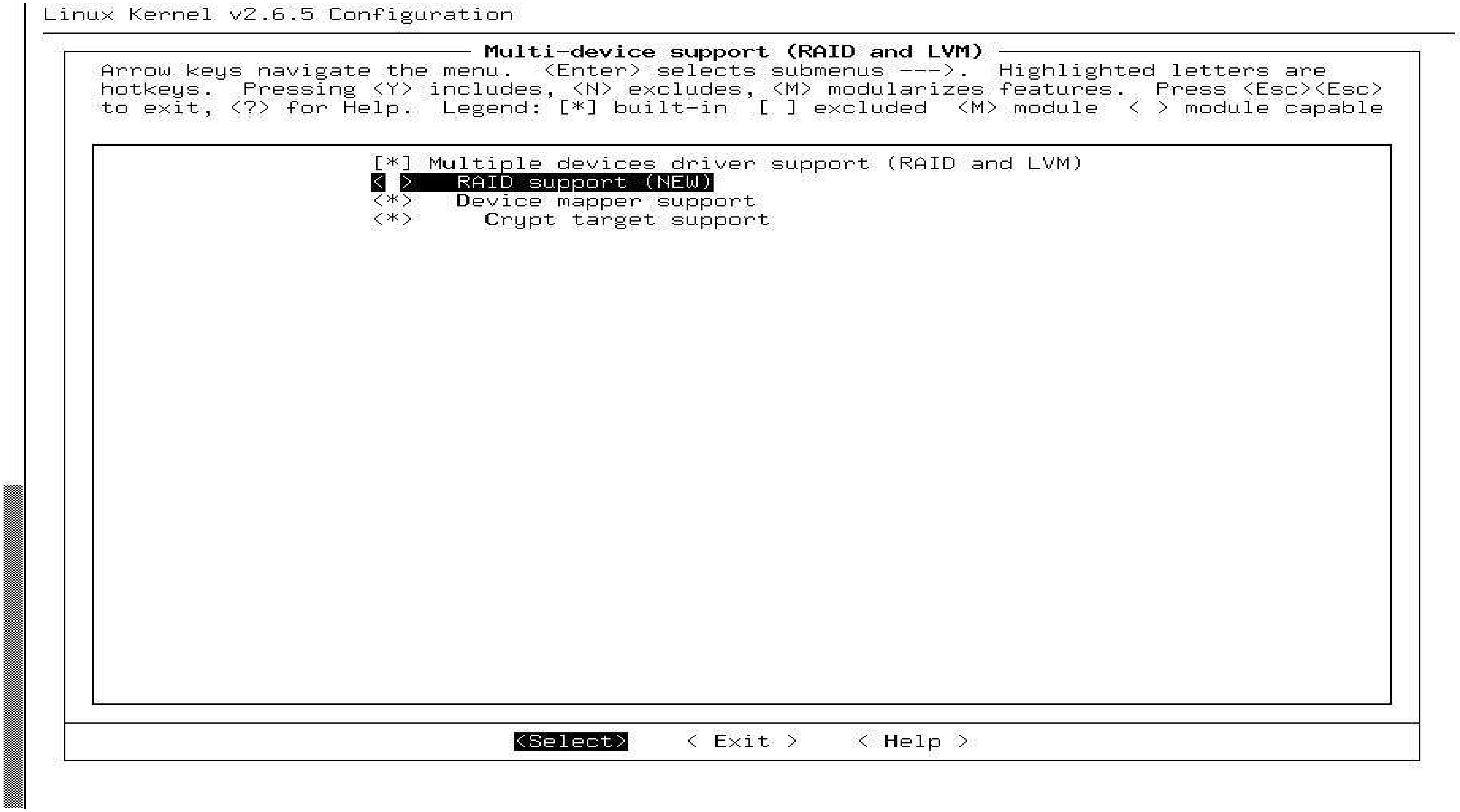
▪ Kernel 2.6.5 - CryptoLoop



```
Linux Kernel v2.6.5 Configuration

                              Block devices
  Arrow keys navigate the menu.  <Enter> selects submenus --->.  Highlighted letters are
  hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc>
  to exit, <?> for Help.  Legend: [*] built-in  [ ] excluded  <M> module  < > module capable

              <*> Normal floppy disk support
              < > XT hard disk support
              <*> Compaq SMART2 support
              <*> Compaq Smart Array 5xxx support
              [*]   SCSI tape drive support for Smart Array 5xxx
              < > Mylex DAC960/DAC1100 PCI RAID Controller support
              < > Micro Memory MM5415 Battery Backed RAM support (EXPERIMENTAL)
              <*> Loopback device support
              <*>   Cryptoloop Support
              <*> Network block device support
              < > Promise SATA SX8 (carmel) support
              < > RAM disk support
              [ ] Support for Large Block Devices

                          <Select>    < Exit >    < Help >
```

IPSec - Linux 2.6 Config

- **Kernel 2.6.5 - DM-Crypt**

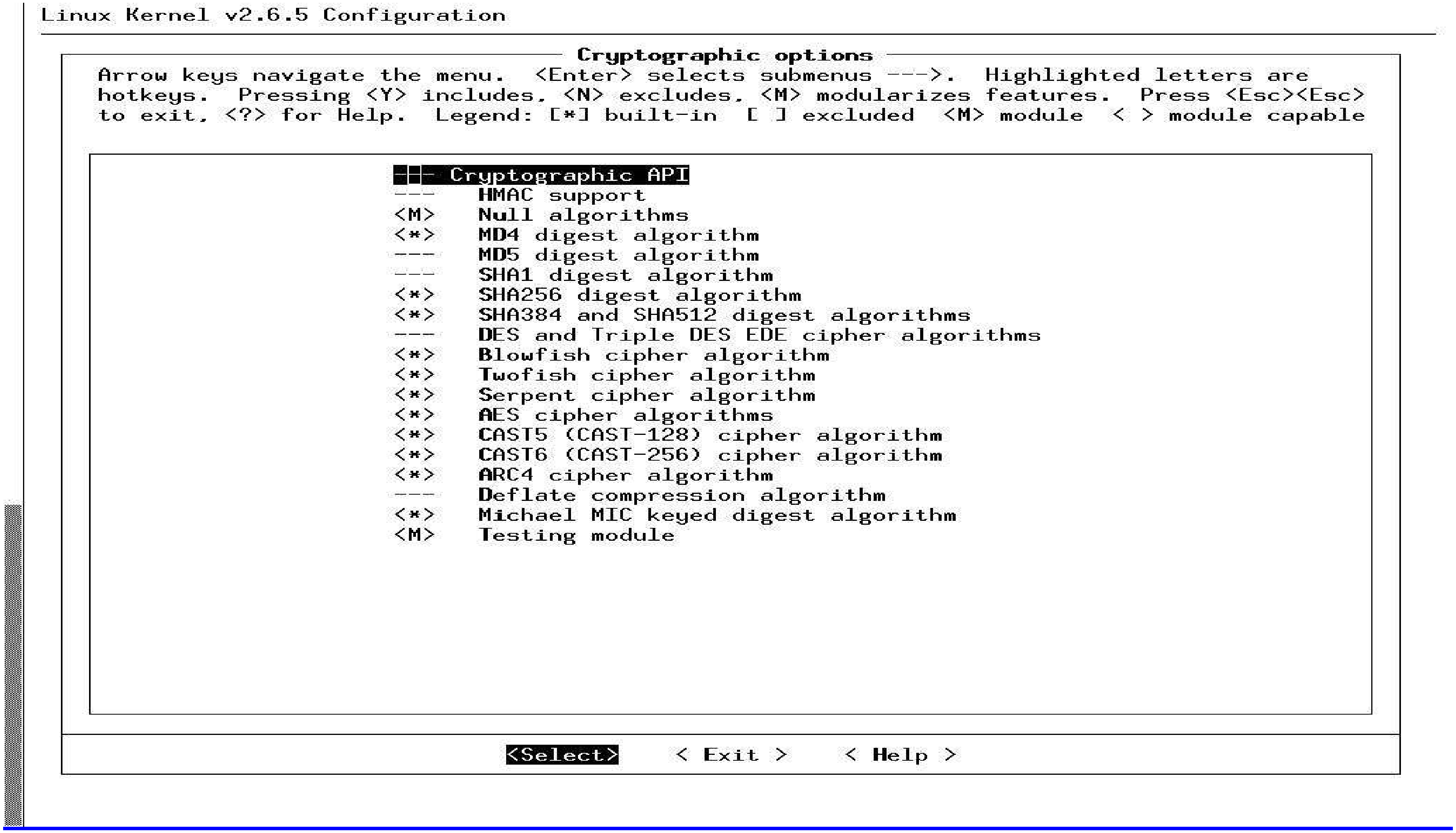


```
Linux Kernel v2.6.5 Configuration

                        Multi-device support (RAID and LVM)
  Arrow keys navigate the menu.  <Enter> selects submenus --->.  Highlighted letters are
  hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc>
  to exit, <?> for Help.  Legend: [*] built-in  [ ] excluded  <M> module  < > module capable

                  [*] Multiple devices driver support (RAID and LVM)
                  < >   RAID support (NEW)
                  <*>   Device mapper support
                  <*>     Crypt target support

                          <Select>    < Exit >    < Help >
```

IPSec - Linux 2.6 Config

Paktronix Systems
Network Security Solutions

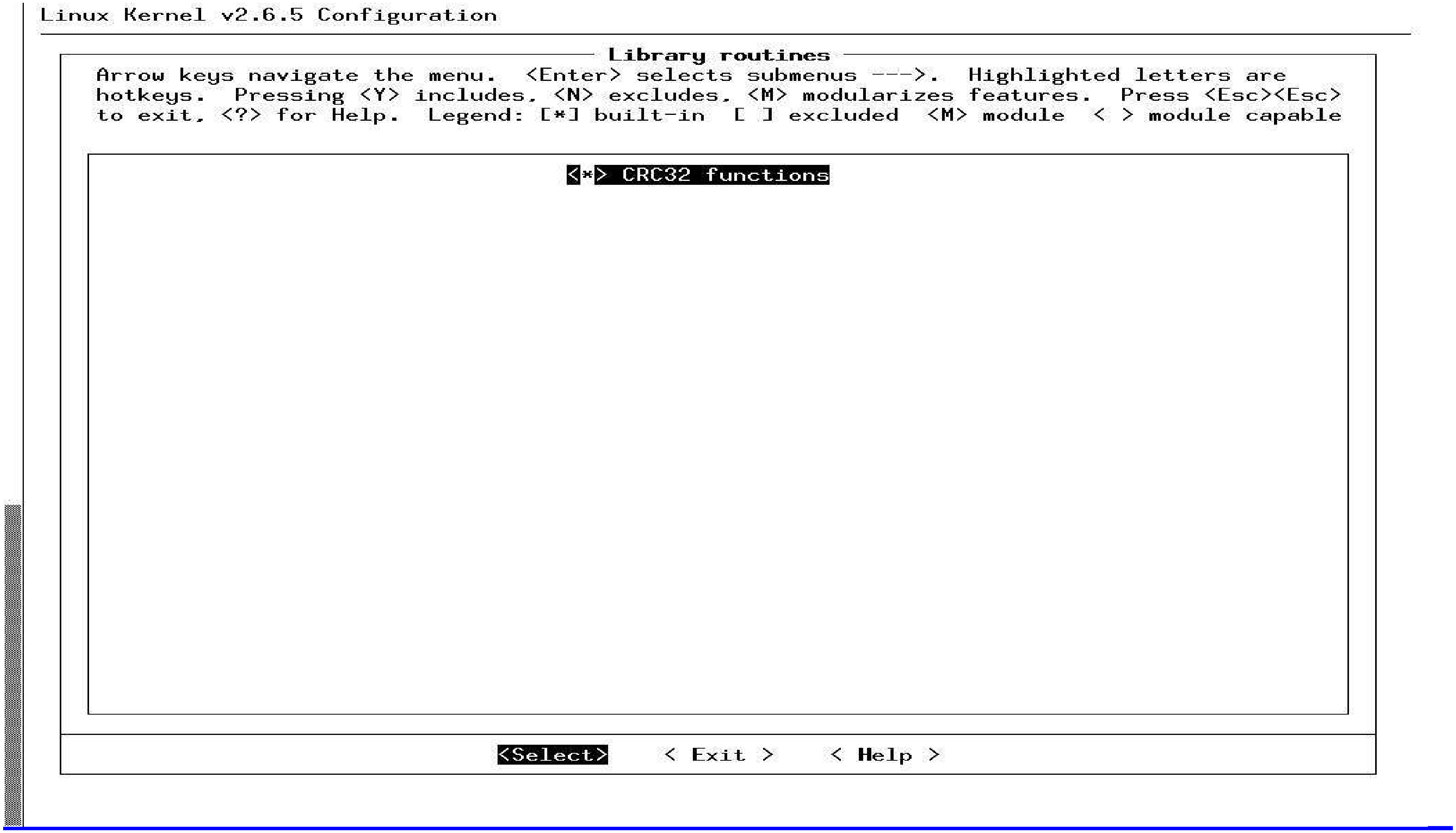
- **Kernel 2.6.5 - CryptoAPI**



```
Linux Kernel v2.6.5 Configuration

                          Cryptographic options
 Arrow keys navigate the menu.  <Enter> selects submenus --->.  Highlighted letters are
 hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc>
 to exit, <?> for Help.  Legend: [*] built-in  [ ] excluded  <M> module  < > module capable

                     --- Cryptographic API
                     ---     HMAC support
                     <M>     Null algorithms
                     <*>     MD4 digest algorithm
                     ---     MD5 digest algorithm
                     ---     SHA1 digest algorithm
                     <*>     SHA256 digest algorithm
                     <*>     SHA384 and SHA512 digest algorithms
                     ---     DES and Triple DES EDE cipher algorithms
                     <*>     Blowfish cipher algorithm
                     <*>     Twofish cipher algorithm
                     <*>     Serpent cipher algorithm
                     <*>     AES cipher algorithms
                     <*>     CAST5 (CAST-128) cipher algorithm
                     <*>     CAST6 (CAST-256) cipher algorithm
                     <*>     ARC4 cipher algorithm
                     ---     Deflate compression algorithm
                     <*>     Michael MIC keyed digest algorithm
                     <M>     Testing module

                      <Select>    < Exit >    < Help >
```

IPSec - Linux 2.6 Config

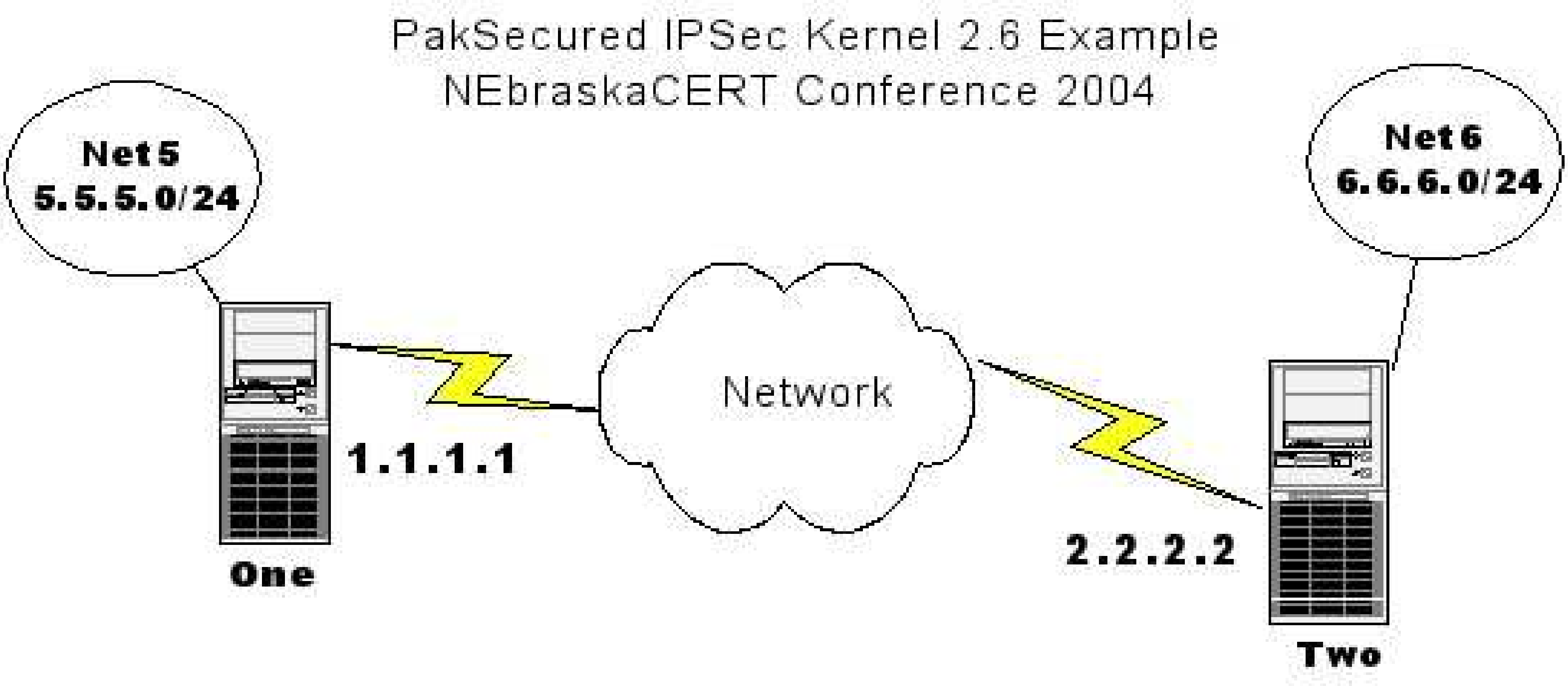
- ## Kernel 2.6.5 - CryptoAPI - 2



```
Linux Kernel v2.6.5 Configuration

                              Library routines
  Arrow keys navigate the menu.  <Enter> selects submenus --->.  Highlighted letters are
  hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc>
  to exit, <?> for Help.  Legend: [*] built-in  [ ] excluded  <M> module  < > module capable

                                <*> CRC32 functions

                         <Select>    < Exit >    < Help >
```

IPSec - MiniHowto

- Mini-HowTo for PakSecured Linux
  - /etc/ipsec contains master configs


PakSecured IPSec Kernel 2.6 Example
NEbraskaCERT Conference 2004
Net 5
5.5.5.0/24
Net 6
6.6.6.0/24
1.1.1.1
Network
2.2.2.2
One
Two

IPSec - MiniHowto

- **Config for System ONE (/etc/ipsec/one.conf)**
  - **Transport Mode setup**

```
flush;
spdflush;
add 1.1.1.1 2.2.2.2 ah 0x200 -A hmac-md5 0x1deadbeefbeefdeadcabbeefed2dead1;
add 2.2.2.2 1.1.1.1 ah 0x300 -A hmac-md5 0x1deadbeefbeeffed1357feeded2dead2;
add 1.1.1.1 2.2.2.2 esp 0x201 -E 3des-cbc 0xfed1111feeded2dead21deadfed2beef111adead2dead111;
add 2.2.2.2 1.1.1.1 esp 0x301 -E 3des-cbc 0x1deadfed2beef222bcabed2222feeded22bcabbfed2dead2;
spdadd 1.1.1.1 2.2.2.2[22] tcp -P in none;
spdadd 2.2.2.2 1.1.1.1[22] tcp -P out none;
spdadd 1.1.1.1[22] 2.2.2.2 tcp -P in none;
spdadd 2.2.2.2[22] 1.1.1.1 tcp -P out none;
spdadd 1.1.1.1 2.2.2.2 any -P in ipsec esp/transport//require ah/transport//require;
spdadd 2.2.2.2 1.1.1.1 any -P out ipsec esp/transport//require ah/transport//require;
```

Config for System TWO (/etc/ipsec/two.conf)

```
flush;
spdflush;
add 1.1.1.1 2.2.2.2 ah 0x200 -A hmac-md5 0x1deadbeefbeefdeadcabbeefed2dead1;
add 2.2.2.2 1.1.1.1 ah 0x300 -A hmac-md5 0x1deadbeefbeeffed1357feeded2dead2;
add 1.1.1.1 2.2.2.2 esp 0x201 -E 3des-cbc 0xfed1111feeded2dead21deadfed2beef111adead2dead111;
add 2.2.2.2 1.1.1.1 esp 0x301 -E 3des-cbc 0x1deadfed2beef222bcabed2222feeded22bcabbfed2dead2;
spdadd 1.1.1.1 2.2.2.2[22] tcp -P out none;
spdadd 2.2.2.2 1.1.1.1[22] tcp -P in none;
spdadd 1.1.1.1[22] 2.2.2.2 tcp -P out none;
spdadd 2.2.2.2[22] 1.1.1.1 tcp -P in none;
spdadd 1.1.1.1 2.2.2.2 any -P out ipsec esp/transport//require ah/transport//require;
spdadd 2.2.2.2 1.1.1.1 any -P in ipsec esp/transport//require ah/transport//require;
```

IPSec - MiniHowto

- **Manual Method Enable**
  - **On ONE:**
    - **setkey -v -f /etc/ipsec/one.conf**
  - **On TWO:**
    - **setkey -v -f /etc/ipsec/two.conf**
- **Done**

IPSec - MiniHowto

- **Automatic Method - IKE/ISAKMP**
  - **KAME IKE daemon RACOON port (ipsec-tools)**
  - **Phase one can use PSK or x509**
  - **Setup racoon conf files ex on ONE:**

```
path pre_shared_key "/etc/ipsec/psk.conf";
remote 2.2.2.2 { exchange_mode main;
        proposal {  encryption_algorithm 3des;
                    hash_algorithm sha1;
                    authentication_method pre_shared_key;
                    dh_group modp1024; }
}
sainfo address 5.5.5.0/24 any address 6.6.6.0/24 any {
        pfs_group modp768;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;}
```

IPSec - MiniHowto

- **Automatic Method - IKE/ISAKMP - con’t**
  - **The example racoon conf implies a setkey of:**

```
flush;
spdflush;
spdadd 5.5.5.0/24 6.6.6.0/24 any -P out ipsec
        esp/tunnel/1.1.1.1-2.2.2.2/require;

spdadd 6.6.6.0/24 5.5.5.0/24 any -P in ipsec
        esp/tunnel/2.2.2.2-1.1.1.1/require;
```

  - **And of course reversed on TWO as appropriate**

IPSec - MiniHowto

- **Automatic Method - IKE/ISAKMP - x509**
  - **Change the example racoon conf to:**

```
path certificate "/etc/certs";
remote 2.2.2.2 {                exchange_mode main;
                                certificate_type x509 "my_certificate.crt" "my_private_key.key";
                                verify_cert on;
                                my_identifier asn1dn;
                                peers_identifier asn1dn;
                proposal {      encryption_algorithm 3des;
                                hash_algorithm sha1;
                                authentication_method rsasig;
                                dh_group modp1024;   }
}
sainfo address 5.5.5.0/24 any address 6.6.6.0/24 any {
    pfs_group modp768;
    encryption_algorithm 3des;
    authentication_algorithm hmac_sha1;
    compression_algorithm deflate; }
```

Thoughts

- **Consider Using SAMBA with IPSec**
  - **Win2K+ systems will converse securely**
  - **Can differentiate security levels**
- **Use NFSv4-TCP with IPSec & DM-Crypt**
  - **DM gives File system protection**
  - **IPSec gives network protection**
  - **NFSv4-TCP gives stability and CIA**
- **CommandLine vs. Certificates**
  - **Which algorithms to use**
  - **WRT SAMBA & NFS -> Admin Privs**

This is The