- **User defined tracking**
    - Found under policy\properties\log and alert tab
    - Custom log filter programs to log screen entries generated by a specific rule
    - Alerts when a complex condition is meet
    - A single rule to generate different types of alarms for a different conditions
    - Written in either C/C+, Bourne Shell, C-Shell or perl
    - ***Alertf*** is the built in tool
    - Place scripts in the $FWDIR/BIN directory
    - Example: Alertf 60 3 fwalert (Alertf – is the command 60 – is the number of seconds that the alerts need to happen in, 3 – is the number of alerts before the command is executed, fwalert is the name of the custom written script)
    - In the rule set Track to "UserDefined"

- **Kernel Components**
    - Kernel Attachment
        - Written for each operating system
        - Inspects each packet passing through the TCP/IP stack, ensuring they have a chance to enter the system
    - Kernel Virtual Machine
        - Executes the INSPECT code to enforce security
        - Can generate logs or alerts
        - Gets its information from the Attachment
    - Kernel Address Translation
        - Translates source and destination IP address
        - TCP/UDP port numbers
        - Sequence numbers for ICMP
        - Special protocol support with address translation, ie FTP commands with port numbers in them
    - Kernel Encryption
        - Encrypt and decrypt data
        - Exchange keys
    - Kernel Logging
        - Transfers log entries, alerts and kernel traps from the kernel to the daemon for further processing
    - Kernel IOCTL handler
        - Commands come from the daemon to the IOCTL (the daemon needs to tell something to the Kernel, it uses ioctl to communicate with the kernel ioctl)

- **Daemon Component** – Does what the kernel cannot do, open a file or initiate an IP packet
  - Daemon Command Handler
    - Receives commands from the deamon.communicator. Calls the code in the command line utilities to execute.
    - Uses strong authentication and encryption to prevent masquerading.
  - Daemon logging
    - Reads it entries from the kernel then acts according
    - If FW is remotely managed it acts as the transfer agent to send files to MC, it logs locally if it fails to reach the MC
  - Daemon Kernel Trap Handler
    - Accepts traps from the Kernel and performs them on behalf of the kernel
  - Daemon IOCTL
    - Has direct contact with Kernel.IOCTL, used when the daemon needs to contact the kernel directly
  - Daemon Inet
    - Listens for information destined for a content services server (CVP) and either runs the CVP or if it running transfers the data to it.
  - Daemon Communicator
    - Used primarily in a distributed management to transfer log entries, commands, alerts and security policy information.

- **FireWall-1 configuration for content security**
  - CVP – Content Vectoring Protocol – port # 18181
  - UFP – URI Filtering Protocol – port # 18182
  - Content security can be implement on the firewall itself without the use of content vectoring server. The security server can match certain schemes and methods that allow HTML weeding and JAVA blocking actions.
  - A rule is set to specify a resource under service, the inspect engine diverts all packets to the CVP server, which performs the security inspection. If the content allowed a second connection is opened to the final destination.
  - Setup:
    - Define a network object for the 3rd party server
    - Define a UFP/CVP server object for the 3rd party server
    - Define a resource to that specifies matching and what type of action should occur
    - Define rules that specify an action for the resource.
  - **HTTP Security Server** – provides URL filtering for control over web access. It is implemented with the use if a URI resource
  - **SMTP Security Server** – this allows for the hiding of internal addresses from outgoing email, strips specific attachment types, drops messages above a given size and rewrites email addresses. It is implemented with the use of a SMTP resource.

  - **FTP Security Server** – provides authentication services and content security based on FTP commands (PUT/GET), file name restrictions and anti-virus checking for files. It is implemented with the use of a FTP resource.
  - Java and ActiveX Stripping – it is implemented with the use of a URI resource.
    - Stripping Java applet tags from HTML pages
    - Blocking Java attacks by blocking suspicious back connections
    - Stripping ActiveX tags from HTML pages

- **Distributed installation with remote management of FireWall-1**
  - 50 stations max for each management server
  - A management server can either be run on the same server as the inspect/FW module itself or a different one. This choice is made during installation.

  - **FW Module**
    - Enforces security policy
    - Report status and log data to it’s management server
    - Runs on NT, SUN, HP, RS/6000, Bay Networks, Cisco and 3Com Routers, and XyLan, Ipsilon Switches
    - Inspection engine uses *State Full* inspection
      - Understands context to determine if communication should be allowed
      - Understands the intent of a given communication by learning from previous communication sessions, and allows it through for the duration of the session.
      - Closes the needed port when the clients session ends
  - **Management Module**
    - Manages object databases, Rule bases and log files
    - Also for concurrent administrative access with varying user rights
    - Runs on NT, SunOS4, Solaris2m Solaris x86, HP-UX, AIX
  - **GUI Clients**
    - **Building objects and rules**
    - **Views logs and FW status**
    - **Runs on WIN 95, 98, NT X/Motif (Sun,HP & AIX)**

- **Licensing**
  - For the Single Gateway Product, there is only one Firewall Module controlled by one Management Console, and they have to be installed on the same machine, meaning there is only one security enforcement point. However, you can still run the GUI client form another desktop. For multiple gateway products there could be multiple enforcement points. For example, Firewall Internet Gateway/25 means you can have up to 25 Firewall modules controlled by one Management Console.

-
- **CPMAD configuration and troubleshooting**
    - Scans the log and alerts sysadmin of malicious or suspicious activity
    - $FWDIR/conf/cpmad_conf
    - MAD_System_mode = on/off
    - MAD_memory,
    - mad_clean
    - Controlled by the log and alert tab in the polices properties
    - It can monitor
        - SYN Attack
        - Anti Spoofing
        - Successive Alerts
        - Port Scanning
        - Blocked Connection Port Scanning
        - Login Failure
        - Successive Multiple Connections
        - Land attacks
    - Is enabled by default
    - If stopped for any reason it can only be restarted by restarting FW1/VPN1
    - If CPMAD exceeds the memory allocated it will exit
    - If you increase the resolution it will use less memory but take more CPU cycles
    - If you increase the clean it will use more memory and less CPU cycles

- **SYNDefender configuration with a security policy**
    - Policy Properties\SYNDefender
    - TCP/IP 3-way hand shake (client sends SYN, Server sends SYN/ACK, Client returns ACK)
    - Designed to shield server from SYN attacks – attacks where servers are flooded with SYN from valid or invalid IP addresses, either way the server is unable to answer them all (either because they are invalid or because there are too many). The queue fills with unanswerable requests and the server crashes.
    - SYN Passive Gateway
        - Has the firewall wait for a response to the servers SYN/ACK before any further connection is made to the server
    - SYN Gateway
        - Opens a connection by sending its own ACK to the server
    - To increase the amount of time the server will wait for a response for the client, change the time out period on the policy properties\SYNDefender tab

- **Services affected by content security**
  - SMTP, FTP, HTTP
  - The daemon listens INET to send the information to the CVP server.

- **Uniform Resource Identifier (URI) content security**
  - HTTP Security Server
    - Controls users ability to reach certain URLs
    - Is implemented by creating a URI resource

- **Asymmetric versus symmetric encryption**
  - Symmetric encryption
    - Uses the same key to encrypt and decrypt data. It is also called shared key encryption.
    - 1000 times faster than Asymmetric encryption
    - Since the same secret key is used from both encryption and decryption, is someone stolen they could decrypt all the data. Keys should be exchanged in a secure manner.
    - Keys should be replaced periodically.
  - Asymmetric
    - Uses one key to encrypt the data and another to decrypt it
    - Is 1000 times slower than symmetric encryption
    - Sometimes called public-key encryption
    - Uses Deffie-Hellman key scheme to create the keys
    - The combination one firewalls public key and another's private create a shared secret key.
    - It is mathematically impossible to derive the secret key from the public key.

- **Tunneling-mode encryption versus in-place encryption**
  - Tunneling Mode
    - Encrypts the packet then encapsulates the packet within the encryption protocol header. It does this by embedding its own network protocol within the packets TCP/IP headers.
    - Supports all algorithms except FWZ-1
    - Encrypts IP and TCP headers
    - Adds a new IP (first) header and IPSEC (second) header in the packet
    - Can be used in a VPN that uses illegal/reserved IP addresses without the needing address translation or proxying
    - Analogy: you write a message (data) and place it in an envelope. You address the outside of the envelope with the destination address and your return address (header). The addressed envelope (packet)

        is then placed inside another envelope that has a different destination address and return address (encryption protocol header)
        - The drawback to this is the packet size increases. This may degrade network performance.
        - This is a higher security solution.
    - **In-Place Mode**
        - Encrypts the payload of the packet only leaving the IP header and TCP header intact.
        - Has better network performance because the size of the packet does not increase.
        - Better performance than IKE, SKIP and Manual IPSEC encryption
        - Used in FWZ-1 ONLY!!!
        - Drawback is the headers remain intact, indicating the origin IP address and destination IP address.

- **SecuRemote and SecureClient**
    - **SecuRemote**
        - Allows for WIN9x and WINNT and W2k clients to access the private network
        - Transparently encrypts any TCP/IP communications.
        - Encrypts data before it leaves a remote computer.
        - Interfaces with any existing adapter and TCP/IP stack.
        - Enables security features, including authentication servers, logging ands alerts
        - Enables access for FW1 SecuRemote users through the Rule Base
        - Includes stronger authentication using Diffie-Hellman and RSA algorithms, as well as strong encryption using FWZ-1 and DES.

    - **SecureClient**
        - Is basically SecuRemote with the added feature of a policy server and the ability to enforce a local policy on the workstation running SecuRemote (a mini-firewall)
        - The client receives its policy from the policy server (also called a security server).
        - It can be used inside the LAN to protect sensitive servers.
        - It can be used outside the LAN to protect the desktop
        - The desktop policy includes the following four options
            - Allow All – allows all communication to and from the SecureClient
            - Allow Outgoing & Encrypted – Allows both outgoing and encrypted communications from the SecureClient as described in the next two polices.
            - Allow Outgoing Only – Allows only SecureClient initiated connections.

        - Allow Encrypted Only – Allows only encrypted communications to or from the SecureClient. If the SecureClient resides in the encryption domain of a gateway, all communication, which remains in the gateway's domain, is trusted and treated as though encrypted.

- SecuRemote Service
    - This service starts when the computer starts up.
    - Loads the SecuRemote kernel with information about all SecuRemote Servers and their encryption domains.
    - Provides a GUI allowing users to add, update and remote sites.
    - Maintains the site lost and assigns a username and password to each site.
    - Exchanges a session key with the SecuRemote Server

FireWall –1/VPN -1 Encryption Schemes

- Manual IPSec
    - Fully manual key management for IPSec

- FWZ
    - Check Point's proprietary key management scheme
    - Provides automated updates of Public Keys
    - Encrypts all data behind the IP and transport (UDP/TCP) header
    - Uses Reliable Data Protocol (RDP) to manage VPN session keys, encryption methods and data integrity
    - Firewalls use Reliable Datagram Protocol (RDP) for an out-of-band session to negotiate session key, to agree on encryption method, and to decide whether MD5 data integrity will be used for that session. In addition, RDP supports an automated and secure way of synchronizing public keys that are not up-to-date
    - Uses in-place encryption which has its data integrity bits inserted into header fields
    - Packet size is fixed
    - Supports FWZ1 48bit which is exportable outside the US

- IKE

    - Standards describing the general framework for encryption and authentication of IP packets
    - Employ DES and Triple DES for encryption, and MD5 and SHA-1 for authentication

        - Can be used manually (Manual IPSec) or with automated key management schemes such as ISAKMP and SKIP
        - IPSec with ISAKMP is mandatory for IP version 6
        - Uses Security Association (SA) to define the security parameters for a specific IP host, including usage of Encryption and/or Data Integrity, Encryption and/or Data Integrity methods and keys. SA itself is identified using a 32bit Security Parameters Index (SPI) that refers to a specific SA value for VPN partners. There are two headers for identifying the relevant SA: Authentication Header (AH), containing the message digest; and Encapsulating Security Payload (ESP), containing a per packet Initialization Vector (IV) for enhancing security
        - SPI should be conveyed to the other party using an external secure channel

    - SKIP
        - Sun's IP layer key management scheme for IPSec
        - Encapsulates the original packet with a SKIP header and IPSec headers
        - Diffie-Hellman key pair for each participating node
        - Uses one fixed SPI (0x1)
        - SecuRemote Client Encryption
        - Enables mobile users to communicate
        - Allows VPLs (Virtual Private LAN) over a single physical LAN

    - **Schemes supported for SeucRemote**
        - IKE
        - FWZ-1

- **Account Management Client**
    - Works with LDAP
    - Based on x-.500
    - Advantages of Multiple LDAP servers – compartmentalization, by allowing a larger number of users to be distributed across several servers, High Availability and remote site can have their own LDAP directory which would speed up access
    - Distinguished Name (DN) - is made by associating the sequence on DN's from the lowest level of a hierarchal structure to the root. Example – "cn= John Brown, o= ABC Company, c=US"
    - To create a site – right click over the red "x" and choose create object
    - Sites cannot be deleted from the GUI. You must do it from the command line, changetype = delete

- **Load balancing components and associated rule bases**
  - Connect Control Module contains the load balancing algorithms
    - Sever Load – Determines the load of each physical server. Server load ***requires*** a load-measuring ***agent*** to be installed on each server. Unsupported servers include, LINUX, HP MPE or AS/400
    - Round Trip – Determines the time a packet takes to make a round trip from the FW to the server. It will PING each server 3 times and use the server with the fastest average.
    - Round Robin – Chooses the next physical server in the server group. FW1 estimates that each server is capable of handling roughly the same load, so when a new request comes in it is sent to the next server in the list.
    - Random – chooses the server at random.
    - Domain – choose the physical server that is closest to the client based on domain name.
  - HTTP Load balancing - uses connect control
  - Other - uses ARP to connect to physical servers
  - Persistent server mode – ensures that once a connection has been made all further communication are handled by the same server. This process saves time and creates accuracy.
  - Two rules need be create to allow load balancing to work. The first rule allows traffic to pass between the user and the logical server. ANY > Logical Server > Service > accept. The second rule allows sessions to be created and continued between the user and the server. ANY > Physical Server > Service > accept.

- **Proper VPN architecture and deployment applications**
  - Security
    - Encryption – scrambles the data so that only those with the proper key can read it.
    - Authentication – Data Authentication ensures the data is the same when it arrives as when it left. User Authentication ensures the user is who they claim to be.
    - Access Control – controls the amount of freedom a VPN user has, and controls the access of partners, employees and other outside users to applications and different portions of the network. It controls access to each network, making sure user has access to what they need and nothing more.
  - Traffic Control
    - Quality of Service control with Flood Gate –1 user's can control which data has priority ensuring proper network performance.

- VPN accelerator card can be used to increase speed by off loading encryption from the CPU.

  - Enterprise Management
    - Allows the organization to define a single, central, enterprise-wide security policy for the entire network.
  - VPN's can be used for;
    - Enterprise-wide intranets
    - Remote access for off-site users
    - Telecommuting programs
    - Branch Office interconnectivity
    - Moving existing applications from a private network
    - Providing backup and overflow capacity for private networks using the internet
    - Overnight system backups
    - Software distribution
    - Virtual project teams
  - Proper Planning should take into account
    - Geographic distribution – a multinational VPN could have export restrictions on the cryptographic algorithms and key lengths that can be used.
    - Importance and Timeliness of Encrypted Data – Analyze data and create a balance between high encryption and speed. Sales data has a higher weight in security and timeliness than 5-year-old data.
    - Future needs – planning for long-range goals early will make expansions simpler and less disruptive.
  - Intranet VPNs – Facilitate secure communication between a company's internal departments and its remote branch offices
  - Extranet VPNs – facilitate secure communication between z company and its strategic partners, customers and suppliers

- **Advanced uses of Client Encryption with VPN-1**
  - **MEP –** If a gateway fails while connections are open, they will automatically reconnect to the backup after a short delay. There for it is not necessary to create sites for each backup location.

- **Single Entry Point (SEP) and Multiple Entry Point (MEP) High Availability solutions**
  - When you assign a gateway to a gateway cluster, any properties previously configured are over written to match the clusters properties.
  - **SEP** – two or more gateways are synchronized so that there is a single entry point from the Internet to the internal network. If one gateway should fail another synchronized gateway will take its place and maintain connections.

- Two networking conditions must be satisfied when implementing a SEP configuration;
  - A mechanism established for redirecting traffic around the failed gateway to the backup gateway.
  - State synchronization between the gateways so that backup gateways are always able to continue connections that were originally handled by the failed gateway.
- Restrictions;
  - Gateways must be running on the same platforms, for example a FW running on NT can not sync with a FW running on Solaris.
  - Gateways must be the same software versions
  - Gateways must have the same security policy installed.
  - The management server of a SEP gateway cannot be installed on the same host as a cluster object.
  - SKIP encryption cannot be used.

- **MEP –** In a MEP there are multiple geographically separated entry points from the Internet to the internal network, with a gateway at each entry point. These gateways are not synchronized.
  - IP pools are used to create ranges of IP addresses that a gate substitutes for the source IP address. This ensures correct routing in asymmetric routing environment.
  - Restrictions;
    - Current MEP configurations only support SecuRemote connections
    - Encryption methods are limited to FWZ and IKE (see above)
    - The management server of a MEP gateway must be located on a remote host
    - All participating gateways must be FW 4.1
    - Participating SecuRemote clients must use 4118 or higher
    - Asymmetric routing – Use IP pools to ensure when a client connects to a gateway; reply packets are routed to that same gateway. If you choose an address range or network that is ‘local; to the gateway internal interface, “Proxy-ARP” must be used on the addresses in the IP pool.
    - Dropped Connections – If a gateway fails while connections are open, they will automatically reconnect to the backup after a short delay.
  - The SecuRemote client with attempt to connect to the primary gateway, if this site is not available, the client will automatically attempt to connect to the gateway that has been configured as the backup gateway during setup.

- **Network address considerations for VPNs**
  - Whether static or dynamic every host in a network has a IP address

    - If you attempt to implement a VPN for networks in which host from one network use any of the IP addresses from the other network, the VPN will fail at some point.
    - Static Addresses – If your network uses static IP address, you will need to ensure that no two addresses are the same in any network.
    - Dynamic Addresses – if you network uses dynamic addressing ensure that you are using IP Pools and the addresses do not overlap.

- **Desktop Policies created and enforced by a Policy Server**
    - Policy Server extends security to the desktop by allowing administrators to enforce a security policy on desktops. This could be both inside the LAN and outside on the Internet. This would prevent authorized connections from being compromised.
    - To use a Policy server in a network you must have;
        - A Policy server from which the SecureClient obtains its Desktop Policy
        - SecuRemote software with the Desktop Security feature installed
        - A special license is also required. This is based on the amount of users allowed to receive a Desktop policy
        - Also sometimes called a Security Server
    - SecureClient
        - Is an extension to SecuRemote that allows desktop users to download Desktop polices from Policy servers.
    - Desktop Policy
        - Only ONE security policy for all SecureClients within a policy server's domain. Any SecureClient machine not using the correct policy will be denied access.
    - Types of Policies
        - Allow all – allows all communication to and from the SecureClient
        - Allow Outgoing and Encrypted – allows both outgoing and encrypted communications from the SecureClient as describes by the next to policies.
        - Allow Outgoing Only – allows only SecureClient initiated connections
        - Allow Encrypted Only – allows only encrypted communications to or from the SecureClient. If the SecureClient resides in the encryption domain of the gateway, all communication, which remains in the gateway's domain, is trusted and treated as though encrypted.

- **Parameters of userc.C file modification**
    - Important for MEP SecuRemote setups (first Three)
        - Active_resolver (true) – if true the SecuRemote client will automatically initiate an RDP status query with a gateway to determine if it is still alive. If false it will not poll the gateway until a connectivity failure occurs, this may cause the user some added delay in reconnecting.

        - Resolver_session_interval (60) – this is the interval in between RDP status queries.
        - Resolver_ttl (10) – this is the number of seconds the SecuRemote client will wait for a reply to RDP before declaring it unavailable.
        - keepalive (false) - Specifies whether the VPN/FireWall Modules will maintain session key information for the Client.
        - keep_alive_interval (n) - When keepalive is true, the Client will ping the VPN/FireWall Module every *n* seconds. keep_alive_interval is relevant for IKE only. For FWZ, the Client will ping every 800 seconds if keepalive is true.
        - dns_xlate (true) - Enable split DNS feature (see "DNS" on page 153) — server must be configured appropriately.
        - dns_encrypt(true) - Enable DNS encryption — server must be configured appropriately.
        - fwm_encrypt (false) - Enable SecuRemote encryption for GUI Client-Server communication — server must be configured appropriately.
        - gettopo_port (264) - Specifies the port for topology download. If unsuccessful after 30 seconds, the Client will try again on port 256.
        - encrypt_db (false) - Obscure topology information in local database.

- **Methods of setting passwords prior to attempting authentication**
    -

- **Over Lapping Encryption Domains**
    - Full Overlap – VPN-1 supports Full Overlap. In a full overlap the encryption domains are identical. To implement great a group that includes both gateways and all networks they protect. They specify that group as each gateways encryption domain. Asymmetric routing can be an issue. Use IP Pools or NAT to ensure proper routing.
    - Partial Overlap – VPN –1 does not support Partial Overlapping domains. This is happens when at least one host is in both encryption domains.
    - Proper subset – This is when one gateways encryption domain is fully contained in another. When a SecuRemote client connects to the inner gateway the rule base of the outer gateway must allow this connection.

- **Asymmetric routing environment issues**
    - Asymmetric routing for reply packets and back connections is a potential problem with fully overlapping encryption domain. A SecuRemote Client can connect to Gateway A, but the host's reply packets could be routed through Gateway B, which is does not encrypt the packet.
    - Use IP pools to ensure when a client connects to a gateway; reply packets are routed to that same gateway. If you choose an address range or network

that is 'local; to the gateway internal interface, "Proxy-ARP" must be used on the addresses in the IP pool.

- **Gateway clustering**
  - Gateway Clusters are a new feature incorporated into FireWall-1 4.1 that allow for High Availability VPNs in combination with third-party High Availability products, which includes the Nokia-based VPN-1 Appliance. It, along with FireWall-1's State Synchronization Mechanism allows for a secondary gateway to be able to process encrypted traffic in the event the primary firewall fails. The Gateway Cluster object can only be utilized if there exists an underlying HA solution. This could be Stonesoft's Stone beat Full Cluster, IPSO's VRRP, Rainfinity's Rainwall, or Check Point's own HA Module. You need to have your management console on a separate platform from the systems that you intend to configure into a Gateway Cluster.
  - A Gateway Cluster is a nothing more than a virtual firewall. It takes two or more firewalls in an HA configuration and makes them appear as a single entity for the purposes of installing a security policy and encryption. Setting up a VPN involving Gateway Clusters is not very different from setting up a VPN involving a single gateway. You will notice that the moment you make a firewall workstation object part of a gateway cluster, many of the tabs in the workstation properties simply disappear. This configuration now needs to be done from the Gateway Cluster object. When you configure the VPN-related parameters for the firewall, you configure them on the Gateway Cluster object, not on the workstation object for the firewalls that are a member of the gateway cluster.
  - To enable Gateway Clusters, you will need to enable them in the Rulebase Properties, High Availability tab. Check the "Enable Gateway Clusters" feature. Once you've done this, you will be able to create a Gateway Cluster. Create the Gateway Cluster object using the VRRP (or other Highly Available) IP address and configure it as you would a workstation object for a VPN. Now go into each of the workstation objects representing the real firewalls and make them a member of the Gateway Cluster. Note that you may need to accept certain things (like the IKE service) to the Gateway Cluster address, but you cannot put the Gateway Cluster object in the rule base. In this case, simply create a workstation object with a different name and the same IP address as the Gateway Cluster. You will get a warning about this. Provided you created the Gateway Cluster address first, you can ignore this error message.

- **IP pools**
  - A potential problem is asymmetric routing for reply packets and back connections. . Suppose a SecuRemote Client connects to a host through Gateway A, but the host's reply packet is routed through Gateway B, which does not encrypt the packet.

    - IP Pools, ranges of IP addresses that a gateway substitutes for the source IP address to ensure correct routing of reply packets (Multiple Entry Points configuration only).

    - An IP Pool is a range of IP addresses (an Address Range, a network or a group of one of these objects) routable to the gateway. When a connection is opened to a host, the gateway substitutes an IP address from the IP Pool for the source IP address. The IP Pool addresses must be routable to the gateway, so that reply packets from the host return to the gateway, which restores the original source IP address and forwards the packets to the source. The IP addresses in an IP Pool are usually illegal. If the IP addresses are legal addresses in the local network, you must use the proxy ARP method to configure the routing so that reply packets are routed back to the gateway. For information on the proxy ARP method, see "Ensuring That the Packet Reaches the Gateway" on page 443 of *VPN-1/FireWall-1 Administration Guide*.

- **Processes and restrictions related to the configuration of SecuRemote within a Multiple Entry Point VPN environment**

- **Processes and restrictions related to the configuration of SecuRemote within a Single Entry Point VPN environment.**

Important Commands

fwconfig

- configures FireWall-1

fw

- together with command line arguments manages the system

fwuninstall

- stops the firewall
- removes FW-1 from the kernel and .rc files
- restores inetd.conf
- does not remove the FW-1 software

fwstart

- loads the Firewall Module
- starts fwd, the snmp daemon, authentication daemons, and fwm

fwstop

- kills fwd, fwm, snmpd, authentication daemons
- unloads the Firewall Module

fw load

- compiles and installs a security policy

fw unload

- uninstalls the currently loaded security policy

fw logswitch

- creates a new log file named fw.log

fw putlic

- installs a FireWall-1 license

fw dbload

- downloads the user database

fw stat

- shows the hosts status

fw log

- displays the log files content

fw ver

- shows the version number of FireWall-1