Contents

Contents 1

Introduction 3

- Cisco Security Management Tools 4
- Control of Data 4
- Security Policy 5
- Risk 6
- System Development Life Cycle (SDLC) 6

Understanding the Risks 7

- Layer 2 risks 8
- Layer 3 risks 9
- Upper Layer risks 11
- Physical 12

Configuring Devices 13

- Basic device Configuration 13
- AAA 15
- User Privileges 17
- Logon Security 18
- AutoSecure and One Step Lock Down 19
- Logging 21
- NTP 22

Layer 2 security 23

- Port Security 23
- 802.1x Port Security / Network Admission Control (NAC) 24
- Storm Control 24
- Span ports (Switchport Analyser) 25
- Securing VLANs 25
- Securing IP at Layer 2 27
- Useful Commands 28
- Best Practices 28

IOS Firewall 29

- Firewall Introduction 29
- Static Packet Filtering 29

CBAC/Classic Firewall 32

Zone based Firewall (ZFW) 32

IPS 35

IPS Introduction 35

Configuring IPS on a Cisco Router using SDM 37

Logging & Monitoring 38

Notes 40

VPN / Cryptography 41

Hashing & Digital signatures 41

Symmetric Encryption 42

Asymmetric Encryption 43

Choosing an encryption method 44

Key Management 44

PKI 45

IPSec 46

Configuring Site to Site VPNs 48

Endpoint Security 51

Endpoint Security Introduction 51

Cisco NAC 52

Cisco Security Agent (CSA) 53

IronPort 53

San and Voice Security 54

SAN Security 54

Voice Security 55

Notes 56

Introduction

IEEE Standards

IEEE No	Use
802.1d	STP
802.1q	Vlan trunking
802.1w	RSTP (Rapid spanning tree protocol)
801.2x	Port based Network Access Control
Ethernet II (DIX v2.0)	Ethernet (with Frame type field)
802.3	Ethernet (With length field)
802.3u	100 Base T
802.3z	1000Base-X (Fibre)
802.3ab	1000Base-T (Ethernet)
802.5	Token Ring
802.11a	5 GHz
802.11b	2.4 GHz (1-6-11 clean channels)
802.11g	2.4 GHz (1-6-11 clean channels)
802.11i	WPA 2

Number Table

128	64	32	16	8	4	2	1
128	192	224	240	248	252	254	255
255	127	61	31	15	7	3	1

Well Known Ports

Protocol	Port	IP
FTP	20, 21	TCP
SHH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
Tacacs	49	TCP
DNS	53	TCP, UDP
DHCP / BOOTP	67	UDP
TFTP	69	UDP
POP3	110	TCP
NEWS	119	TCP
NTP	123	UDP
SNMP	161, 162	UDP
Radius	1645 / 1812	UDP

Definitions

Term	Description
NIPS	Network IPS
HIPS	Host based IPS

Hardening a system	Remove known system vulnerabilities by upgrading, patching and disabling unneeded applications and services
Bastion Host	A host which is placed in a vulnerable position such as a PC running a firewall. It is therefore expected to be hardened.
Blended Threat	An attacker uses multiple means of propagation such as viruses with worm like capabilities.
Rainbow Tables	A list of plain text strings and the corresponding (ND5 / SHA) hash. This allows an attacker to quickly find plaintext which would generate the required hash even though the plaintext would more than likely differ from the original hashed text.
Password salting	One or more bits are changed in a password, the avalanche effect will result in a completely different hash reducing the risk of cracking using rainbow tables.
IP Directed broadcast	An IP packet whose destination address is a valid broadcast address for some IP subnet which originates from a node that is not itself part of that destination subnet
Anti-X	Anti Virus, Anti Spam etc.

Cisco Security Management Tools

Security Device Manager (SDM) – A java/web based tool to configure and manage standalone routers

Cisco Security Monitoring, Analyses and Response System (MARS) – Appliance based reporting and logging solution to correlate network events from all devices to identify threats. It is able to notify and reconfigure networks to reduce the impact of the threat. Risk of False positives is reduced as MARS correlates data from multiple sources.

Cisco IDS Event Viewer (IEV) – Java based no cost solution for viewing and managing up to five IPS/IDS sensors. IEV supports SDEE communication with the sensor. IEV is currently being replaced with the Cisco IPS Express Manager (IME).

Cisco Security Manager – A powerful GUI management platform to manage a Cisco based network containing up to thousands of devices. CSM is capable of managing many Cisco devices (ASA, HIPS, VPN etc).

Control of Data

Typical data classifications include military – Unclassified, Sensitive But Unclassified (SBU), Confidential, Secret & Top Secret.

US Government data classification levels – Confidential, Secret & Top Secret.

Roles in data storage / use –

- Owner – Ultimately responsible for the data, select custodians, decides the classification and reviews the data.
- Custodian – Day to day responsibility for the data such as backups, reviews of security settings etc.
- User – No responsibility classification of the data but is responsible for the correct use o the data according to operational procedures.

Security Controls –

- Administrative – Controls policies and procedures including security awareness training, security policies and standards, change controls, audits etc.
- Technical – Controls the electronics, hardware, software etc. Includes IPS, VPN, Firewalls, OTP systems, authentication servers etc.
- Physical – Intruder detection, security guards, locks, UPS, Fire control systems etc.

Each control can be broken down into three sections, Preventative, Deterrent and Detective.

Response to Security Breaches
To prosecute an attacker the following things must be established-

- Motive – Compile a list of individuals with motive to perform the attack.
- Opportunity – Did the individuals have the opportunity to perform the attack.
- Means – Did the suspected attackers have the technical knowhow and tools to perform the attack.

Goals for security –

- Confidentiality – Ensure the data is confidential, example is a reconnaissance attack, the attacker wants to gather confidential information without being noticed such as data, access passwords. Encryption is a useful method to ensure confidentiality.
- Availability – Example attack is a DoS attack.
- Data integrity – Ensure the data is not changed during a transfer & the data origin is authentic (e.g. man in the middle attack)

Aims – Creation of a dynamic (monitor, revise & adapt to latest risks) security policy

Cisco's Deference in Depth – Implement multi layer network defences ASA/Firewalls, NIPS, HIPS (Cisco Security Agent), Out of Band management.

Cisco Self-Defending Network – A suite of security solutions to identify threats, prevent threats and adapt to emerging threats. It consists of two key components, Cisco Security Manager and Mars (Monitoring, Analysis and Response System) to monitor and control network security devices and tools such as IOS & ASA firewalls, IPS sensors, NAC & Cisco Security Agent.

Disaster Recovery –

- Hot Site – A complete redundant site with comparable hardware and a very recent copy of the data. To swap over only the latest data changes need to be applied. This allows recovery in seconds or minutes.
- Warm Site – A redundant site but the hardware is configured and does not contain the data. This requires physical access to the site to configure the systems and as a result can take days to bring on line.
- Cold Site – A site with core facilities (power, WAN links, racks etc) but no computing equipment. To bring online routers, switched, servers etc need to be acquired before setting up. Can take weeks to bring online.

Security Policy

A defined policy for informing users (Acceptable Use Policy), specify mechanisms for security and to provide a security baseline.

A policy can contain –

- Standards – Define the standards used by the organisation at a high level.
- Guidelines – A list of suggestions and best practices, typically defined by national security agencies & institutes.
- Procedures – In depth procedures with step by step instructions on how to perform day to actions. Essential to ensure consistency.

Risk

Risk Analysis methods-

Quantitative – Uses a mathematical model to derive a monetary cost of losses per annum which can then be used to justify countermeasures.

- Asset Value (AV) – Value of the asset including purchase price, implementation costs, maintenance costs, development costs etc.
- Exposure Factor (EF) – An estimated percentage of loss/destruction that would occur in an event. This could by around 50% for example as provided the software and data is backed up offsite the loss would only be hardware.
- Single Loss Expectancy (SLE) – This is the expected monetary loss for a single occurrence of a threat. SLE = AV * EF.
- Annualised Rate of Occurrence (ARO) – The expected annual frequency of the event.
- Annualised Loss Expectancy (ALE) – Total expected loss per annum. ALE = AV * EF * ARO.

Qualitative – A scenario based model used for large risk assessments where calculating the quantitative risk is impractical due to the quantity of assets.

System Development Life Cycle (SDLC)

Phases-

- Initiation – Insists of definition of the potential impact should a breach of security occur and an initial risk assessment,
- Acquisition and Development – Consists of a more in depth risk assessment, security functional & assurance analysis, cost considerations
- Implementation – Inspections, acceptance, system integration, security certification.
- Operations and Maintenance – Configuration management & control and continuous monitoring.
- Disposition – Information preservation (keep the data stored on the system), media sanitisation and disposal.

Understanding the Risks

Hacker	Purpose
Black Hat	Profit financially from hacking others
White Hat	To test network security, usually their own – ethical
Grey Hat	Combination of the above two
Phreakers	Hack to make cheap / free phone calls
Hacktivist	Further their cause/ beliefs
Script Kiddy	Not true hackers but download tools from the internet to perform hacks
Academic Hacker	Attempt to hack to further their education (steal other peoples assignments or amend grades)
Hobby Hacker	Purely hobby, not intending to cause any harm.

Attack Category	Description
Passive	Gather information / reconnaissance. Very difficult to detect
Active	Actively trying to break into a system or leaving malicious payloads. This is easier to detect as the attacker must be actively sending traffic
Close-in	Typically external person manages to physically connect to the inside of the network to perform an attack
Insider	People who are employed by a company trying to hack the internal systems/data
Distribution	Software/hardware developers deliberately leave “backdoors” in their systems to allow future access
Attack Type	**Description**
Reconnaissance	Gathering information for a future access / DoS attack
Access Attacks	Attempt to steal information
Denial of Service	Attempt to break things (destroyers, crashers, flooders). The attack will either crash the system or make it unresponsive to legitimate use.
Social Engineering	Befriend an internal employee to exploit their position (give out network details, passwords, launch unauthorised VPN tunnel)
Privilege escalation	Exploit a software vulnerability (such as buffer overflow) to gain higher authorisation. Two forms, horizontal where an attacker tries to access information for other users on the same level or vertical where the attacker tries to gain higher (administrative) privileges.
Security method	**Description**
Firewalls / ASA	
Anti – X	Anti-Spyware, Anti-Virus, Anti-Spam etc
IDS	Sits outside of the ‘forwarding oath’ looking for and reporting problems
IPS	Sits inside of the ‘forwarding oath’ looking for, reporting and filtering problems

Hacking Approach

1. Reconnaissance – Learn about the system by performing port scans etc (also known as ‘footprinting’)
2. Indentify applications and operating systems. Use this information to find vulnerabilities.
3. Gain Access, social engineering is the most common method by persuading somebody to give out their login details.
4. Login with user credentials then escalate privileges.
5. Gather / create additional usernames and passwords in case the original username is removed.

6. Create a Backdoor to allow future access, in case main point of attack entry is shutdown.
7. Use the system – Steal data, cause denial of service etc.

Layer 2 risks

Reconnaissance (Packet Capture) – Use of tools such as Wireshark to pull data off the wire.

Denial of Service (CAM Overflow Attack - MAC Flooding Attack) – An attacker floods the switch with frames containing different source MAC addresses. Once the CAM is full the switch enters a failover mode where the switch treats all frames as a broadcast, in effect acting like a hub. Packet sniffers could now sniff confidential data as data packets are now sent out of all ports. Additionally this can cause the switch and network bandwidth to become saturated. The risk can be reduced using dot1x and some/all of the commands-

```
(config-if) # switchport port security                                  - Enable port security
(config-if) # switchport port security maximum 2                        - Set maximum MAC address
(config-if) # switchport port security mac-address 1234.5678.abcd       - Define a static MAC address
(config-if) # switchport port security mac-address sticky               - Enable sticky learning
```

NOTE – Above example syntax is in italic and description in normal font.

VLAN Hopping Attack (Double Tagging) – A frame can be double tagged with two separate VLAN ID's. If the first tag is the same VLAN as the Native VLAN / access port VALN the first tag will be stripped off leaving the second tag. This tag will be the destination VLAN of the VLAN hopping attack, when received by a second switch this packet will be forwarded out the destination VLAN. Setting the native VLAN of trunks to a VLAN not used this can remove this risk.

Conditions for a successful attack-

- The attacker must be connected to an access port
- The VLAN configured on that access port must be the native dot1q vlan.

VLAN Hopping Attack (Rogue Switch) – Some Cisco switches are set to trunk mode 'dynamic desirable' on all switch ports, if a rogue switch is connected to a port a trunk will dynamically be created (using DTP) giving access to all VLANs. Additionally it is possible to get a host to send DTP packets in order to create a trunk with a switch.

To stop the risk all non trunking ports should be set to an access port, setting mode to auto is not sufficient. Additionally trunking ports should be placed into unconditional trunking mode and DTP disabled-

```
(config-if) # Switchport mode trunk
(config-if) # Switchport nonegotiate
```

STP Root Bridge Attacks – A rogue switch configured with a lower BID can become the root bridge on the network. This could cause inefficient traffic flow or in a worst cases if this switch is connected to two different points in the network some or all of the LAN traffic will go through the rogue switch. Two methods exist to reduce the risk.

If Rootguard is configured on a switch port and a superior BPDU is received on that port the port will go into 'root-inconstant' state and not transmit traffic. Once the superior BPDU stop the port will transition through the STP state (Listening, Learning, Forwarding). This is typically enabled on all ports on the chosen root switch.

(config-if) # spanning-tree guard root

If BPDUGuard is configured on a port and any BPDU is received the port will be placed into 'err-disable' state.

(config-if) # spanning-tree bpduguard enable

Alternatively bpduguard can be automatically enabled on all portfast ports using-

(config) # spanning-tree portfast bpduguard default

MAC Address Spoofing – A rouge host could transmit a packer with a source MAC Address of another host. The CAM table will be updated to send traffic destined to the original host to the rogue host. This can be avoided using port security.

Layer 3 risks

Man in the Middle Attack (Gratuitous ARP) – A gratuitous ARP message is typically sent out when an IP Address or MAC address changes. This forces all connected devices to update their tables to reflect the changes. Typically used a fail over situations such as server clustering, if the active server / LAN card fails a gratuitous ARP message is sent out to inform all clients of the new MAC address of the new active server / LAN card. This can be exploited for example if a rogue hosts sent a gratuitous ARP packet out replacing the MAC address of the default gateways IP address, all traffic destined for a gateway could be sent to the host instead. This can be mitigated using dynamic ARP inspection.

Man in the Middle Attack (rogue DHCP server) – A rogue DHCP server is introduced into the network which could give out incorrect DNS and default router IP addresses. The incorrect address could result in network traffic passing through the attacking host in an attempt to gain confidential data / password etc. DHCP Snooping will remove the risk of unauthorised DHCP servers.

Denial of Service Attack (DHCP Pool Exhaustion) – A rogue host could make multiple DHCP requests (each with a different MAC address) which will use up the allocated DHCP pool. This can be stopped by enabling port security with a maximum number of MAC address and using the command-

(config-if) # ip dhcp snooping limit rate x

Denial of service (TCP SYN flood) – The attacker send many packets to the victim with the SYN flag set, sometimes using spoofed source IP addresses. This exhausts the server resources (too many half open connections) eventually leading to a denial of service. TCP Intercept in intercept mode will complete the TCP connection (send an ACK and SYN back to the originating host), if the connection initiates successfully then the router will open a TCP connection to the server and merge the two connections. Watch mode only watches connection requests and close incomplete requests after a certain time. TCP intercept also monitors the total number of half open connections, if this rises over a high watermark the router will enter aggressive mode and start to close half open connections as new connections attempts occur and the timeout for closing connections will be reduced, in an attempt to reduce the number of half open connections further. This continues until a low watermark is reached.

Mode	Description	Command Syntax
(config)	Set the mode to 'watch'	Ip tcp intercept mode watch
(config)	Set timeout before resetting the connection attempt	Ip tcp watch-timeout *seconds*
(config)	Set the mode to 'intercept' mode	Ip tcp intercept mode intercept
(config)	Define ACL for traffic to monitor/protect	Ip tcp intercept list *aclno*
(config)	Set the drop mode when aggressive mode	Ip tcp intercept drop-mode {oldest | random}
(config)	Set high incomplete TCP connections for aggressive mode (1100 default)	Ip tcp intercept max-incomplete high *number*
(config)	Set low incomplete TCP connections for aggressive mode (1100 default)	Ip tcp intercept max-incomplete low *number*

NOTE – For the command syntax, parameters are italicised.

Reconnaissance (Ping/ICMP Sweep) – Used to find live IP addresses. If a host if found an attacker can launch a port scan.

Reconnaissance (Port Scan) – Scans all ports to find open ports on a single host.

Reconnaissance (Port Sweep) – Scans multiple hosts for a single open port (eg 80).

Denial of service (Ping of Death) – A containing a large amount of data (some even larger than the limit of an IP packet 65535) is sent to a host. Although this will be fragmented as it crosses through the internet, when reassembled, a server could crash or suffer corruption.

Denial of service (Ping Flood) – A number of pings hit an attacked target, these take up inbound bandwidth, processor resources to process then addition outbound bandwidth replying to the pings.

Denial of service (Smurf Attacks) – An attacker broadcasts an echo request packet using the IP address of the victim host. As many hosts will receive this echo request they will all reply to the victim server causing a potential DoS. This can be avoided if the devices are configured not to replay to pings sent to a broadcast address. Additionally 'no ip directed-broadcast' (default on 12.x IOS) should be configured.

IP Spoofing – A host impersonates a valid network device Ip address to-

- Send malicious code into the network.
- Trick other hosts to send confidential data to the rogue host.
- Part of a reconnaissance attack.

Two Methods-

Non Blind (Same subnet). The sniffs the network for and attempts to find the TCP sequence number of a TCP session. The hacker can then ACK the connection and spoof the IP connection.

Blind (Not same subnet / separated by routers). To reduce the risks inbound packets must be filtered (ingress filter).

Packets with a source addresses defined in RFC3704 (RFC2827) should be filtered

- 0.0.0.0
- 10.0.0.0/8 (RFC1918)
- 172.16.0.0/12 (RFC1918)
- 192.168.0.0/16 (RFC1918)
- 127.0.0.0/8
- 224.0.0.0/4
- 240.0.0.0/4 (RFC1918)

IP Source routing – This allows a sender to define the route used by the packet on outbound and inbound traffic. This is enabled by default, to turn off use the command '*no ip source-route*'.

Upper Layer risks

Password Attacks – Find password using-

- **Brute Force** – Every password combination is attempted to gain access. This can take a long time and can be mitigated by setting the maximum failed login attempts and login blocking delays on the router.
- **Dictionary** – A dictionary of common words is used. A password policy to include numbers and symbols in passwords is advised, ideally not at the end or the start of the password.
- **Trojan Horses & Key loggers** – Malicious code on a device to capture passwords and other data.

Salami Attack – A number of small actions that do not in themselves cause damage but combined have a greater effect.

Trust Exploitation – Indirect attack, rather than directly attack the target, attack an easier host which has a trust relationship with the target. This can then be used as a stepping stone to the target.

Data diddling – Changing data before or during input or storage,

Worm – Spreads automatically throughout the network by looking for vulnerabilities in systems.

Virus – Cannot spread by itself, it requires help from a user to propagate such as forwarding an infected file etc.

Trojan Horse – This appears to be a regular program but contains a malicious payload. Many contain a backdoor allowing remote access to an infected system.

Buffer Overflow – A buffer overflow occurs when something inject/sends more data to a device that is larger than the buffers size. This can overwrite an applications data and cause a crash or overwrite the return address in the stack allowing malicious code to be run. Typically buffer overflow attacks are used to gain escalated privileges through root escalation / rooting the system.

Physical

- Lock Doors (Card reader, pin entry system)
- Tested UPS devices on network devices
- Temperature monitoring
- Proper disposal of equipment and documentation to avoid 'dumpster diving' where a hacker could acquire systems, IT documentation etc)
- Wiretapping, physical access to cables allowing electronically retrieving data passed over them. Usually with voice traffic.
- Wireless Sniffing.
- Social Engineering.

Configuring Devices

Basic device Configuration

Creating a Banner

(config) # Banner motd $ - $ is the delimiter
This is Router 1$
(config) # Banner login $ - $ is the delimiter
Please leave now if you are unauthorised$

The *login* banner appears after the *motd* banner but before the login prompt. The Exec banner appears after logging in. It is possible to use tokens in the banner text which will be replaced with the actual value. Banner message Tokens-

- $(hostname)
- $(domain)
- $(line)
- $(line-desc)

Configure SSH access

Telnet is unencrypted so using SSH is advised.SSH requires either a local user database or AAA configured as SSH does not support passwords directly created on the VTY lines.

Mode	Description	Command Syntax
#	Show SSH config	Show ip ssh
#	Show logged in users	Show users
(config)	Create a user with level 7 pwd	username admin password <password>
(config)	Create a user with a secret pwd	username admin secret <password>
(config)	Required to generate certificate	ip domain-name <domain name>
(config)	Generate the encryption keys	crypto key generate rsa
(config)	Generate the encryption keys	crypto key generate rsa general-keys modulus *bits*
(config)	Optional - set SSH version 2	ip ssh version 2
(config)	Number of login retries	ip ssh authentication-retries *x*
(config)	Set timeout of a SSH connection	ip ssh time-out *seconds*
(config)	Enter VTY config mode	line vty 0 4
(config-line)	Set valid VTY protocols	transport input ssh
(config-line)	Set VTY to use local database	login local
(config-line)	If using AAA use this	login aaa

NOTES-

- SSH settings in SDM can be found in the ‘Additional Tasks’ section under ‘Router Access. This has a button ‘Generate RSA Key’.
- SSH2 is more secure but not as widely supported as SSH1.
- ‘Ip ssh time-out *seconds’* command only refers to the length of time taken to perform the login procedure. Once logged in ‘exec-timeout’ takes effect.
- Recommended minimum key length is 1024 bits

Enable SDM

Requires Java

SDM can either be installed to a router, PC or both. The PC Version gives a richer UI with more power. If installed on a router some .tar files containing the Java code will be copied to the routers flash.

The SDM installer also has a set of base configuration files that will be copied to the routers flash for use in the event of the user using SDM to revert the router back to factory settings. This config will perform the initial setup of the router and enable SDM access.

Mode	Description	Command Syntax
(config)	Create a user in the local username database	username admin privilege 15 secret *password*
(config)	Enable http server *	ip http server
(config)	Set http to use the local username database	ip http authentication local
(config)	Set the domain name of the router. Rqd for RSA *	Ip domain-name *domainname*
(config)	Generate the encryption certificate *	Crypto key generate rsa general-keys
(config)	Enable the http secure server *	Ip http secure-server
(config-line)	Configure the vty lines. Required to install SDM	Line vty 0 4
(config-line)	Set VTY to use the local user db. Rqd to install)	Login local
(config-line)	VTY login will be set to level 15 (NOT REQUIRED)	Privilege level 15

- Typically either HTTP of HTTPS will be configured, not both.
- Line VTY command are not required for SDM use but are required for SDM installation.

IOS Resilient Configuration

These commands copy the IOS image and config to a hidden area in flash (requires a large CF card for the IOS image). This is called a bootset.

(config) # secure boot-image	- Make a resilient copy of the IOS image
(config) # secure boot-config	- Make a resilient copy of the current config
# show secure bootset	- Verify the bootset
(config) # secure boot-config restore flash:/test	- Restore the config to a file on flash.
(config) # no secure boot-config	- Disable boot config. Must be connected to the console

Password Recovery

To stop access to rom monitor mode use the command-

(config) # no service password-recovery

It is no longer possible to use the rom monitor functions to change the config register or xmodem an IOS into flash. I is still possible to use 'break' at bootup and after confirming the prompts the startup config will be erased entirely.

AAA

What Is AAA

- **Authentication** - Authenticates the user. AAA can be used for PPP, VTY, Console, AUX VPN.....
- **Authorisation** - defines what the user can do.
- **Accounting** - logs actions performed by the user.

AAA Sources

- **Local Database (Self Contained AAA)** – Local '*username xxx password xxx'* database.
- **RADIUS**
- **TACACS+**

Access Modes

- **Character** – Used for remote administrative access to VTY,TTY, Aux and Console. AAA can be configured for login, exec and enable.
- **Packet** – Used for Remote network access on async, BRI ec. AAA will be configured ppp for network.

RADIUS

Industry standard solution (IEFT) allowing basic, combined user authentication and authorisation (different privileges not supported). Passwords are sent encrypted but all other communication is clear. UDP based. Radius cannot control the user level privilege.

TACACS

Cisco Secure Access Control Server (ACS) for Windows or ACS Appliance. Cisco proprietary solution allowing complete Authentication (using internal or other databases such as Novell or Active Directory), Authorisation levels (time of day, resource restrictions, connection limits, command limits) and Accounting (CSV or ODBC). All communication is encrypted. TCP based.

The authentication process is completely controlled by the ACS Server. The router will ask the ACS server for the username prompt, it then prompts the user with this prompt. Once entered the router will forward the username to the ASC Server and ask ACS for the password prompt, again this is prompt is sent to the user. One the user has entered the password this is sent to the ACS server for authorisation. The ACS server will send one of the following responses-

- Accept
- Reject
- Continue – The ACS server needs more information to authenticate the user.
- Error – An error has occurred in the authorisation process.

Configuring

Mode	Description	Command Syntax

#	Display current privilege level of user	Show privilege
#	Show AAA authentication statistics	Show aaa sessions
#	Show tacacs server config	Show tacacs
#	Show radius config	Show radius {local-server | server group |stat | table}
#	Debug AAA authentication events	Debug aaa authentication
#	Debug tacacs events	Debug tacacs [events]
#	Debug radius events	Debug radius
(config)	Turn on AAA globally	Aaa new-model
Setup Local		
(config)	Create a local username database entry	Username name secret pwd
(config)	Set maximum failed attempt before locking out user	Aaa local authentication attempts max-fail count
#	Clear a locked out user	Clear aaa local user lockout *username*
Setup Radius Client		
(config)	Set the source IP for packets	Ip radius source-interface *interface*
(config)	Set a server ip address	radius-server host *ipaddr*
(config)	Set server with a specific key	radius-server host *ipaddr* key *key*
(config)	Set a key for all radius servers	radius-server key *key*
Setup Tacacs Client		
(config)	Set the source IP for packets	Ip tacacs source-interface *interface*
(config)	Set a server ip address	Tacacs-server host *ipaddr* single-connection
(config)	Set server with a specific key	Tacacs-server host *ipaddr* single-connection key *key*
(config)	Set a key for all tacacs servers	Tacacs-server key *key*
Setup Authentication Method Lists		
(config)	Create a login default authentication list	Aaa authentication login default <method list>
(config)	Create a login named authentication list	Aaa authentication login *name* <method list>
(config)	Create an enable auth list (default only)	Aaa authentication enable default <method list>
(config)	Create a PPP default authentication list	Aaa authentication ppp default <method list>
(config)	Create a PPP named authentication list	Aaa authentication ppp *name* <method list>
Authorization		
(config)	Create a default authorisation list	Aaa authorization exec default <method list>
(config)	Create a named authorisation list	Aaa authorization exec *name* <method list>
Aaa accounting		
(config)	Create an default accounting list for level 15 commands	Aaa accounting commands 15 default start-stop <method list>
(config)	Create a default accounting list for exec sessions	Aaa accounting exec default start-stop <method list>
Apply a method list to VTY lines		
(config-line)	Apply a default authentication list to a line	Login authentication default
(config-line)	Apply a named list to a line	Login authentication *name*
Apply a method list to a PPP connection		
(config-if)	Set CHAP authentication using the default PPP method list	Ppp authentication chap default

Aaa new-model disables all traditional authentication methods (*password* and *login* command under vty lines etc). At a minimum a local username must be created to avoid locking yourself out of the device.

Authentication Methods (method list)

Up to five methods can be specified in the method list (4 for SDM). When used the list is checked from the first entry to the last entry but only if previous method fails (timeouts or fails). If an authentication process succeeds but the user is denied on other methods are checked. Possible methods-

- Enable – Use enable password for authentication.
- Group – Use specified server-group (radius / tacacs+)
- Line – Use line password for authentication.
- Local –Use local username authentication.
- None – No authentication. There will be no login prompt.

Example

```
(config) # Aaa new-model                                          - Changes to new aaa method
(config) # Tacacs-server host 10.20.0.2 single-connection         - Configure a TACACS server
(config) # Aaa authentication login default group tacacs+ local   - Set tacacs with a fall back of local
(config) # Aaa accounting commands 15 default start-stop group tacacs - log Level 15 commands
(config) # line vty 0 4
(config-line) # login authentication default
(config) # Aaa authentication login NOLOGIN none                  - Set no login
(config) # line con 0
(config-line) # login authentication NOLOGIN                      - Turn off password on console
```

NOTES-

- AAA can secure anything requiring a username/password such as PPP Lines, VPN, VTY lines, Dialup Modems, Console & Aux access etc.
- As soon as the '*aaa new-model'* command is entered, all lines will be automatically configured to use the local database. Make sure a local database user has been created to remove risk of being locked out of a device.
- By default the 'default' AAA method list is set to use the local database. The default method list is used for all lines etc unless another method list is specified.
- When using AAA for the enable password, as the username is not requested devices use a username of '$enab15$' which must be configured on the AAA/Radius server.
- AAA can be configures in SDM using the 'AAA' settings under the 'Additional Tasks' functions.

User Privileges

Privilege Level Access

Commands can be made unavailable/available to lower privilege users using the 'privilege' command-

(config) # Privilege *mode* [all] {level *level command* | reset *command*}

Where mode is the configuration mode. E.g. exec, configure, interface etc.

```
(config) # privilege exec level 5 show          - Only allow level 5 and above access to show commands
(config) # privilege exec level 5 ping          - Only allow level 5 and above access to ping commands
(config) # privilege interface level 5 ip address
(config) # privilege interface level 5 ip
(config) # privilege configure level 5 interface
(config) # privilege exec level 5 configure
```

```
#enable secret level 5 TEST
#enable 5
```

Role Based Access

Assigning IOS commands to Privilege levels can be used to give different users different access but as a command can only be assigned to one level it is complicated to configure. Role Based Access on the other hand does not have this restriction and allows creation of restricted administrative accounts (sub-administrator) with specifically defined privileges (CLI Views). To create a view the ‘root view’ must be enabled.

Commands mode {include | include-exclusive | exclude} [all] command

Configuring

```
(config) # aaa new-model                              - Enable AAA (required)
(config) # aaa authorization exec default local       - Set the authorisation to local (required)
# enable view                                         - Enable the root view
(config) # parser view LIMITEDMODE                    - Create the view
(config-view) # secret test                           - Set a password for the view
(config-view) # commands exec include ping            - Allow the ping command
(config-view) # commands exec include all show        - Allow show commands with wildcard
#show parser view all
```

Superviews

```
# enable view
(config) # parser view SPV superview
(config-view) # secret test
(config-view) # view LIMITEDMODE
(config-view) # view LIMITEDVIEW
```

Using the views

```
# enable view LIMITEDMODE                                      - Manual / Testing
```

or

```
(config) # Username LIMITEDUSER view LIMITEDMODE secret test   - Create a user to use this view
```

Notes-

‘Commands exec include all’ enables wildcard for the following command

Logon Security

Block logins for 15 seconds after 3 failed logons. The ‘log’ will enable logging to a Syslog server

```
(config) # security authentication failure rate 3 log
```

Set the minimum password length.

```
(config) # security passwords min-length 6
```

NOTE - Only applies to newly entered passwords, not existing passwords

Encrypt all clear text passwords in the config

(config) # service password-encryption

NOTE - is a level 7 encryption which is easily cracked (Vigenere encryption). Using 'enable secret' is recommended for enable password as it uses a stronger MD5 hash.

Automatically logout a session after 1 minute 30 seconds
(config-line) # exec-timeout 1 30

Securing VTY Lines

# Show login

Block logins for 120 seconds after 3 failed logins in 60 seconds
(config) # login block-for 120 attempts 3 within 60

NOTE - This could be used for a denial of service attack – stopping all access to the router by permanently blocking it out.

Allows access from the IP address specified in the ACL even if the login is blocked out
(config) # login quiet-mode access-class 10

Delay between successive failed login attempts.
(config) # login delay 10

Generate a Syslog message after 3 failed attempts or every successful logon attempt.

```
(config)#login on-failure log every 3          - Every x is optional
(config)#login on-success log every 1          - Every x is optional
```

AutoSecure and One Step Lock Down

AutoSecure

Interactive – Similar to setup mode '*auto secure full*'.

Non-Interactive – Automatically lock down router to Cisco recommendations. Potentially could be too secure . To configure use '*auto secure no-interact'.*

Changes-

- Finger disabled
- PAD disabled
- UDP & TCP Small Servers disabled
- BootP disabled
- HTTP Services disabled
- CDP disabled
- NTP disabled
- Source Routing disabled
- Proxy ARP disabled on interfaces
- IP Directed broadcasts disabled on interfaces
- MPO (Maintenance Operations Protocol) disabled on interfaces
- ICMP Redirects disabled on interfaces

- Unreachables disabled on interfaces
- Mask Reply messages disabled on interfaces
- Password encryption enabled
- TCP Keepalives enabled
- Logging buffer size is set
- Sequence numbers and timestamps enabled
- CEF enabled
- Reserved IP address ranges are blocked as source addresses on outside interfaces
- Default route to null0 is configured is no default route is already present
- TCP Intercept is enabled
- AAA Enabled
- Set minimum password length and failure rate
- Console log
- Login and password applied to VTY, AUX and CON lines
- Banner is created
- SNMP is disabled depending on prompt or settings – gives opportunity to configure SNMPv3

NOTES-

- Introduced with IOS 12.3

SDM One-Step Lockdown & Security Audit

This performs similar actions to the Auto-secure IOS command, accessed under 'Configure' / 'Security Audit'

Security Audit – SDM will audit the security of the router and give list of vulnerabilities. The user is prompted to secure individual vulnerabilities with descriptions/help. Additionally a drop down is provided to 'Undo Security configurations' on individual security lockdowns.

One Step Lockdown – SDM will perform secure all security vulnerabilities automatically.

NOTES-

SDM differs from Auto Secure by the following-

- Does not disable NTP
- Does not enable TCP Intercept
- Does not configure AAA
- Does not configure three separate ACL to block commonly spoofed source addresses
- SDM will disable SNMP but not provide options for S NMPv3

Logging

Console – By default all logging is displayed on console sessions.

VTY Lines – Logging to a telnet session can be enabled using the command '*terminal monitor*'.

SNMP – Simple Network Management Protocol. Three core components-

- SMNP Manager – The tool which queries, analyses and presents the data on devices.
- SNMP Agent – The monitored device itself.
- Management Information Base (MIB) – The dictionary of object identifiers (OID) available on the device. Each OID is a variable/counter that can be read or set.

SNMP Messages-

- Get – Read only access is sufficient.
- Set – Read/Write access is essential. This is very dangerous facility, it could allow an attacker to gain access to a device if not locked down.
- Trap – The device will send a trap message to the manager component to alert particular issues

SNMP Versions-

- SNMPv1 – Simple to configure. All SMNP traffic is sent in clear text. Counters are limited in value so high bandwidth interfaces could over range counters.
- SNMPv2c – Simple to configure. All SNMP traffic is sent in clear text. Similar to SMNPv1 but counters are capable of much larger values.
- SMNPv3 – Addresses weaknesses of the earlier versions by including authentication, privacy and access control. SMNPv3 operated in one of three modes (noAuthNoPriv, authNoPriv & aithPriv) using MD5/SHA to provide authentication and DES, 3DES or AES to provide the privacy. This is complicated to setup particularly as SDM cannot be used to configure SNMPv3.

```
(config) # snmp-server community public ro           - Configure SNMP community with read only access
(config) # snmp-server community CCSTRING rw 50      - Configure SMNP community with RW & ACL
```

Logging Buffer – All login messages can be saved to memory for later review. '*login buffered 4096'* for example will set aside 4096 bytes to store a log history. '*show log*' will display the login entries.

SysLog

```
(config) # logging hostname <ipaddress / hostname>       - Set Syslog server location
(config) # logging <ipaddress / hostname>                - Set Syslog server location (alternative)
(config) # logging trap <level>
```

Logging Levels

Message will be logged for the level selected and all lower levels.

Emergencies	System is unusable	(severity=0)
Alert	Immediate action needed	(severity=1)
Critical	Critical conditions	(severity=2)
Errors	Error conditions	(severity=3)

Warnings	Warning conditions	(severity=4)
Notifications	Normal but significant conditions	(severity=5)
Informational	Informational messages	(severity=6)
Debugging	Debugging messages	(severity=7)

NOTES

- *'login synchronous'*
- Logging can be found in 'Additional Tasks' then 'Router Properties' in SDM.

NTP

For accurate logging (syslog etc), digital certificates and AAA accounting an accurate time source must be set, NTP can provide this. A router can act as a NTP client, server or peer (bidirectional time transfer).

The recommended approach is to use a public NTP server as the master source, it an NTP server is run internally it is advisable to create an ACL to stop external devices accessing the NTP server.

NTP Client

```
(config) # ntp server x.x.x.x prefer          - Set the time source with optional prefer statement
```

NTP master

```
(config) # ntp master                          - Enable NTP Master
(config) # ntp authenticate                    - Optional, enable NTP authentication
(config) # ntp authentication-key 1 md5 NTP    - Optional, set key number 1 to NTP
```

NTP Peer

This must be defined both sides to define the peer relationship

```
(config) # ntp peer x.x.x.x
```

NOTES-

- NTP Authentication works differently to the norm. The client authenticates the server rather than the server authenticating the client. This prevents the NTP master being spoofed and supplying incorrect time.
- NTP settings in SDM can be found in the 'Additional Tasks' section under 'Router Properties'.
- Ensure the NTP port (UDP 123) is open (ACL)
- Stratum 0 – Atomic clock, Stratum 1 – Time server directly connected to an atomic clock.
- A Server can also Broadcast / Multicast time updates, (routers do not relay these packets).
- An attacker could attempt to change the time in a router which will render digital certificates invalid.
- Using NTP Version 3 or higher for additional security features (encryption etc).

Layer 2 security

Port Security

Mode	Description	Command Syntax
#	Show port security summary	Show port-security
#	Show security for an interface	Show port-security interface *interface*
#	Display the MAC address table	Show mac address-table
(config-if)	Set access port (stops dynamic trunking)	Switchport mode access
(config-if)	Enable port security on port	Switchport port-security
(config-if)	Set violation action	Switchport port-security violation <protect/restrict/shutdown>
(config-if)	Set the maximum mac addresses on port	Switchport port-security maximum *number*
(config-if)	Set static MAC address security	Switchport port-security mac-address *xxxx.xxxx.xxxx*
(config-if)	Port will learn the address & add to config	Switchport port-security mac-address sticky
(config-if)	Aging time for dynamic learned mac addrs	Switchport port-security aging time *minutes*
(config-if)	Set aging time basis	Switchport port-security aging <absolute / inactivity>

Violation modes

- Protect – Allow authorised hosts through but disallow unauthorised hosts
- Restrict – As above but log (SNMP & Log) unauthorised hosts
- Shutdown – Shutdown the port (err-disabled)

NOTES-

- Default maximum MAC addresses is 1. Must set to 2 for daisy chained IP Phone & PC.
- Default violation mode – shutdown (err-disabled).
- Cannot use port security on trunk ports (must explicitly set to an access port), Etherchannel ports, Destination Span ports and 802.1X ports.
- To clear err-disabled issue a ‘shutdown’ & ‘no shutdown’ commands to the interface.

Configure SNMP Traps for MAC Table Event Notification

```
(config) # mac address-table Notification                 - enables feature
(config) # snmp-server enable traps Mac-notification
(config-if) # snmp trap Mac-notification <added /  removed>    - Set interface
```

802.1x Port Security / Network Admission Control (NAC)

Securing a port using 802.1x requires both host (supplicant) and switch ports (authenticator) to be configured with 802.1x EAPOL (Extensible Authentication over LANs). 802.1x requires a Radius server (authentication server).

The physical port on s supplicant is broken down into two logical ports (controlled and uncontrolled) by 802.1x. The uncontrolled port can only pass EAPOL, STP & CDP protocols. Once authentication is successful the controlled port can pass all data.

Dot1x port control modes-

Force-authorised (default) – Any host connected to this port will be considered authorised. In effect no authentication.

Force-unauthorised – Connected hosts will be considered unauthorised.

Auto – This enables dot1x on the port. The port will be unauthorised until the EAPOL packets are exchange then the port will enter an authorised state.

EAP

EAP-MD5

EAP-TLS

PEAP (MS-CHAPv2)

EAP-FAST

Example

```
(config) # aaa new-model                                      - Required
(config) # aaa authentication dot1x default group radius local
(config) # dot1x system-auth-control                          - Enable dt1x globally
(config) # interface fastethernet 0/4
(config-if) # dot1x port-control auto
```

Storm Control

This feature can raise a trap or shutdown an interface is a certain percentage of a ports' traffic is a particular type. As an example, storm control can shutdown a port if it receives excessive broadcasts.

Mode	Description	Command Syntax
(config-if)	Set the action is a storm control tolerance is exceeded	Storm-control action <shutdown / trap>
(config-if)	Set the tolerance for broadcast traffic (% of bandwidth)	Storm-control broadcast level *level*
(config-if)	Set the tolerance for multicast traffic (% of bandwidth)	Storm-control multicast level *level*
(config-if)	Set the tolerance for unicast traffic (% of bandwidth)	Storm-control unicast level *level*

Span ports (Switchport Analyser)

Span will mirror all traffic from a source port or ports to a destination port (sometimes called the monitor port) on either the same switch or across a trunk to a different switch.

Local SPAN – Destination and source ports are on the same switch.

```
(config) # monitor session 1 source interface fastethernet 0/1
(config) # monitor session 1 destination interface fastethernet 0/2
# show monitor                                                    - Display configure monitor sessions
```

Vlan SPAN (VSPAN) – The source is a Vlan.

Remote SPAN (RSPAN) – A dedicated vlan will be created to trunk mirrored packets across a trunk link between two switches. All intermediate switches between the units having the source and destination ports must be RSPAN capable devices.

Source config-

```
(config) # vlan 100
(config-vlan) # remote-span
(config-vlan) # exit
(config) # monitor session 1 source interface fastethernet 0/1
(config) # monitor session 1 destination remote vlan 100 reflector-port  fastethernet 0/10
```

Destination config-

```
(config) # monitor session 1 source remote vlan 30
(config) # monitor session 1 destination interface fastethernet 0/10
```

Notes-

- A source port can be monitored on multiple simultaneous SPAN sessions.
- A source port can be a part of an etherchannel.
- A port cannot be both a source and destination of a monitor session.
- A port can be a destination for only one SPAN session.
- A Destination port cannot be part of an etherchannel
- A Destination port does not run STP, CDP, VTP, PaGP, LACP or DTP.
- Trunk ports can be source and destination ports.

Securing VLANs

Filtering Intra-VLAN Traffic

An ACL on a multilayer switch can be used to filter inter vlan traffic but not intra-vlan traffic. To filter traffic between two hosts on the same vlan a VLAN Access List (VACL) is used.

Only one VACL can be applied to a vlan

To restrict 172.10.10.1 – 3 from accessing any hosts on the 72.10.10.0 network-

```
(config) # ip access-list extended NOACCESSACL
(config-ext-nacl) # permit ip 172.10.10.0 0.0.0.3 172.10.10.0 0.0.0.255  - Used to specify the addresses to match

(config) # vlan access-map NOACCESSVACL 10
(config-access-map) # match ip address NOACCESSACL
(config-access-map) # action drop
(config-access-map) # exit

(config) # vlan access-map NOACCESSVACL 20                               - Consider a match any
(config-access-map) # action forward
(config-access-map) # exit

(config) # vlan NOACCESSVACL vlan-list 1                                 - Apply it to a VLAN
```

Note rule 20, this allows un-matched traffic to be forwarded, without all traffic would be dropped (similar to the implicit deny all on ACLs).

Private VLANs

PVLANs provide layer 2 isolation between ports within the same broadcast domain. There are three types of PVLAN ports-

- **Promiscuous** — A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.
- **Isolated** — An isolated port has complete Layer 2 separation from the other ports within the same PVLAN, but not from the promiscuous ports. PVLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic from isolated port is forwarded only to promiscuous ports.
- **Community** — Community ports communicate among themselves and with their promiscuous ports. These interfaces are separated at Layer 2 from all other interfaces in other communities or isolated ports within their PVLAN.

Community PVLAN – Hosts can communicate with other hosts in a secondary vlan and with the primary vlan but not with hosts in other secondary VLANs.

Isolated PVLAN – Hosts can communicate with the primary vlan but no other host in the and secondary vlan.

VTP must be in transparent mode to create private vlans.

```
(config) # vlan 200
(config-vlan) # private-vlan <isolated / community>
```

Securing IP at Layer 2

DHCP Snooping

This is a method for protecting against unauthorised or rogue DHCP Servers. These can be used to give out an incorrect gateway address, which could cause a host to send all network traffic through an unauthorised router enabling traffic sniffing etc. DHCP Snooping allows all switch ports to be placed in to a trusted or untrusted mode, if a DHCP offer is received on an untrusted port the port will be err-disabled. Additionally DHCP Snooping can be used to rate limit the number of DHCP requests

```
(config) # ip dhcp snooping                  - Enable
(config) # ip dhcp snooping vlan 10  - Enable on additional vlans. Vlan 1 enabled by default
(config) # interface fastethernet 0/3
(config-if) # ip dhcp snooping trust  - Set interface as trusted

(config-if) # ip dhcp snooping rate 10        - Set a maximum rate for DHCP requests to 10 per second
```

NOTES-

- This can be difficult to configure in a multi-switch environment as all inter switch link interfaces (trunks) must be set as trusted.
- Once globally enabled on a switch all ports are set to untrusted. It is therefore important to manually enable trusted ports as required for the DHCP infrastructure.

Dynamic ARP Inspection (DAI)

ARP Cache Poisoning / ARP Spoofing

ARP Spoofing occurs when a host send an ARP request out onto the network requesting the mac address for a particular ip address. A rogue host could respond to the request before the legitimate host which would result in an incorrect mac address in the first host. All traffic now sent between the two hosts will now be sent to the rogue host which in turn forwards to the legitimate host forming a man in the middle attack.

This uses the database created by the DHCP Snooping feature and this forms trusted mapping database. If a switch receives an ARP request on an untrusted port and the MAC-IP mapping is in the trusted mapping database then that ARP request is forwarded. If the MAC-IP mapping is not in the trusted database the ARP request is dropped.

If a port is configure as a Dynamic ARP trusted port the ARP request is forwarded regardless.

```
(configure) # ip arp inspection vlan 10              - Enable on vlan 10
(config) # interface fastethernet 0/1
(config-if) # ip arp inspect trust                   - Set as a trusted port
 # show ip arp inspection
```

The recommendation is to sett all ports connected to hosts as untrusted and all ports connected to other switches as trusted. As ARP packets are inspected on ingress each arp packet will only be inspected once.

IP Source Guard

This prevent a host using another hosts Ip address and like Dynamic ARP Inspection requires DHCP Snooping to be enabled. An untrusted port will only accept DHCP packets until it receives an IP address. This address is recorded and will only accept traffic from that IP address. This reduces the risk of IP Spoofing.

Useful Commands

Mode	**Description**	**Command Syntax**
#	Show all mac addresses	Show mac address-table
#	Show only dynamic learnt address	Show mac address-table dynamic
#	Show address for a particular vlan	Show mac address-table dynamic vlan *vlanid*
(config)	Select a range of interface	interface range f0/6 - 10

Best Practices

- Use secure management (SSH, OOB, Access-class on VTY lines).
- Make an audit sheet (portfast, bpduguard etc).
- Try to reduce the use of VLAN 1 and don't use it as the native VLAN.
- Disable dynamic trunking (set all non trunking ports as access ports).
- Lock down SNMP (Set ACLs, keep community strings secret, avoid RW access).
- Unused port recommendation-
    - Disable the port (shutdown)
    - Set the port to an assess port (switchport mode access)
    - Assign the port to another Vlan (switchport access vlan 99)

IOS Firewall

Firewall Introduction

Firewall Types

Stateless – Use of static packet filters (ACLs) to control what traffic can enter a network. As much network traffic uses random port numbers (FTP, in bound HTTP traffic etc), this method is not optimum.

Stateful – Monitors the state of connections storing them in a session/state table. Storing open connections allows the firewall to detect attacks by examining the sequence numbers (TCP Only) and allows return traffic for outbound connections. A Stateful firewall will not allow a TCP packet with the SYN bit set and only allows packets with the ACK bit set if there is an entry in the session table indicating an inside user initiated the connection. Operates at OSI layers 3, 4 & 5.

Application Layer Gateway – Acts as proxy. Operates at OSI layers 3, 4, 5 & 7. An ALG can enforce user authentication rather than devices

Transparent Firewalls – Transparent firewalls are layer 2 devices which act like a network bridge. They are easily introduced as IP addressing of the existing networks do not need to be changed. Extended ACLs can be created for IP traffic and EtherType ACLs for non IP traffic. By default only ARP traffic can pass. Transparent Firewalls do not pass traffic with an EtherType greater than or equal to 0x600 (CDP, IS-IS etc.). Spanning Tree BPDUs, EIGRP, OSPF etc are supported.

Layered Defence Strategy

1. Perimeter
2. Communications Security
3. Core network Security
4. Endpoint Security

Cisco IOS Firewall feature set

- IOS Firewall – CBAC & Zone Based firewall.
- IPS
- Authentication Gateway – Allows creation of security profiles on a per user basis. Uses Radius or Tacacs servers to store the profiles.

Static Packet Filtering

Description	Identifier	Typical syntax
IP Standard	1-99	Access-list *number* <permit/deny/remark> *source* <log>
Standard expanded range	1300-1999	
IP Extended	100-199	Access-list *number* <permit/deny/remark> <protocol> <source> <dest> <comparison> <port> <log>
Extended expanded range	2000- 2699	
MAC Address list	700-799	

ACL Types

- Standard – Filter only on the source IP address. Typically used for controlling access to VTY lines, NAT etc rather than filtering.
- Extended – Filter on protocol, both source and destination IP addresses and source and destination ports. Typically used for filtering.
- Named – Alternative way of creating and managing all access lists. Lists can be named rather than just numbers and it is possible to edit ACLs as each line of the ACL is assigned a number.
- Reflexive / Established – Opens an inbound traffic rule based on an outbound TCP connections. Similar to the established rule.
- Time-based – Access list enabled/disabled at a particular time.
- Dynamic ACL – Lock and Key. An access list is modified to allow traffic if a user telnets in to the router.

Examples

- Access-list 1 deny 192.168.5.100 0.0.0.0
- Access-list 1 deny any
- Access-list 1 permit host 192.168.3.4
- Access-list 1 permit host 192.168.3.4 log
- Access-list 1 deny 192.168.5.0 0.0.0.255
- Access-list 1 permit any
- Access-list 2 permit 0.0.0.0 255.255.255.255
- Access-list 150 deny ip 192.168.10.50 0.0.0.0 192.168.3.50 0.0.0.0
- Access-list 150 deny tcp 192.168.10.50 0.0.0.0 any eq 80
- Access-list 100 deny ip host 192.168.10.50 192.168.2.0 0.0.0.255
- Access-list 100 permit ip any any

- *!--- Deny special-use address sources.*
- *!--- Refer to RFC 3330 for additional special use addresses.*
-
- `access-list 110 deny ip host 0.0.0.0 any`
- `access-list 110 deny ip 127.0.0.0 0.255.255.255 any`
- `access-list 110 deny ip 192.0.2.0 0.0.0.255 any`
- `access-list 110 deny ip 224.0.0.0 31.255.255.255 any`
-
- *!--- Filter RFC 1918 space.*
-
- `access-list 110 deny ip 10.0.0.0 0.255.255.255 any`
- `access-list 110 deny ip 172.16.0.0 0.15.255.255 any`
- `access-list 110 deny ip 192.168.0.0 0.0.255.255 any`

Named access lists

Mode	**Description**	**Command Syntax**
(config)	Create / edit a standard ACL	Ip access-list standard <*no / name*>
(config-std-nacl)	Create an entry	Permit *sourceaddr*
(config)	Create / edit an extended ACL	Ip access-list extended DENY_HOSTA
(config-ext-nacl)	Create an entry	Permit tcp host *sourceadr* host *sourceaddr*
(config-ext-nacl)	Create an entry with a line no	15 permit tcp host 192.168.10.50 host 4.2.2.4

(config-ext-nacl)	Create a reflexive entry	Permit tcp any any established
(config-ext-nacl)	Delete an existing access list line	No 15
(config)	Re-sequence an ACL	ip access-list resequence *aclno/name startno interval*

Apply a list to an interface / line

Mode	Description	Command Syntax
(config-if)	Apply access list to an interface	Ip access-group *number* <in / out>
(config-line)	Apply access list to a VTY line	Access-class *number* <in / out>

Show commands

Mode	Description	Command Syntax
#	Show interface info (inc ACL)	Show ip interfaces
#	Show all access lists	Show {ip} access-lists
#	Show a specific access list	Show {ip} access-lists *number*

Turbo ACLs

High end routers (7200, 7500 routers and 12000 Gigabit Switch routers) have the ability process ACL quicker. If the Turbo ACL feature is enabled, ACLs are compiled into a lookup table which allows for much faster processing. ACLs with about four or more lines will see a speed improvement / reduction in CPU load.

(config) # access-list compiled	- Enable Turbo ACLs
# show access-lists compiled	- Displays the Turbo ACL state for all ACLs

ACL States

- Operational
- Unsuitable – ACL Cannot be compiled. Turbo ACL cannot be used for dynamic ACLs and time based ACLs.
- Building – Currently building.
- Deleted – There are no ACLs in this entry
- Out Of Memory

NOTES

- A packet filtering firewall operates at layers 3 & 4.
- Use Notepad to write ACLs then copy and paste into the router.
- Use the ‘*reload in 3*‘ command before applying an ACL to an interface. The router will reload itself in the specified number of minutes unless the command ‘*reload cancel*’ is issued. This avoids unintentionally locking yourself out of the device.
- To change a line in a named ACL, the line must be removed using the ‘*no x*’ command then re-added.
- A packet filter typically only filters the first fragment of a fragmented packet as the later fragments will not contain a TCP header.
- Make sure console messages are visible (‘terminal monitor’ if using VTY lines) while implementing/changing ACL just in case an ACL takes some routers functionality out.
- Packets generated by a router are not subject to ACL filters.

- Have an inbound ACL denying with a same source address range as the internal IP addresses to protect against IP Spoofing. Additionally it is recommended to black traffic from RFC1918 addresses, 0.0.0.0 and 255.255.255.255 to prevent broadcast attacks.
- It is advised to allow the following IMCP traffic back in to the router from the internet-
    - Echo-reply
    - Time-exceeded
    - Packet-too-big
    - Traceroute
    - Unreachable

CBAC/Classic Firewall

- Provides Stateful packet inspection, alerts and logging.
- Outbound traffic is inspected up to the application layer in order to check validity and to open corresponding holes in the inbound filter for the return traffic. In addition to per application filtering, both generic TCP & UDP traffic can be inspected to allow returned packets. Generic inspection does not support protocol specific features such as random ports (SIP, FTP etc).
- Has the ability to monitor control channels of protocols such as FTP/SIP to allow opening of correct dynamic UDP/TCP ports.
- Inbuilt defence against TCP SYN and IP Spoofing attacks.
- For the inspection process to work there must be an Extended ACL applied to the inbound direction while outbound traffic can be either standard or extended. This allows Dynamic ACL entries to be added to allow returned traffic back in. The dynamic ACL entries are removed when the TCP session is closed or after a timeout.
- IP Inspection does not apply for traffic generated by the router unless ‘router-traffic’ is used as an option on the ‘ip inspect’ commands.

Example-

```
(config) # ip inspect name FW http          - Create an inspection rule names FW for http traffic
(config) # ip inspect name FW tcp           - Enable TCP generic inspection
(config) # ip inspect name FW udp           - Enable UDP generic inspection
(config) # ip inspect name FW timeout 60    - Set UDP timeout value.
(config) # interface fastethernet 0/1
(config-if) # ip inspect FW out
```

Zone based Firewall (ZFW)

- Released with IOS 12.4(6)T
- Policies are applied between zones (Zone pair)
- All traffic between zones is denied by default unlike access lists which allow all until configured. An exception is the ‘self’ zone where traffic is allowed to pass by default unless explicitly denied
- An interface can only belong to one Zone
- Traffic can flow between interfaces in the same zone
- Traffic cannot flow between a zone and a non zone interface
- Cannot combine zone based and legacy firewall inspection

- Uses a Deep Packet Inspection to catch dynamic port number protocols such as BitTorrent & IM applications.
- SDM will prompt for a DNS config if not already configured as the rules it creates include domain names such as yahoo instant messaging servers.
- Hosts connected to an interface will be a part of the zone assigned to that interface. The IP Address of the interface itself is assigned to the 'self' zone.

ZFW Actions

- **Inspect** – Allows the traffic through but inspect the packet to ensure the data is not malicious
- **Drop (deny)** – Does not allows the packet to pass. It is analogous to an ACL deny statement.
- **Pass (permit)** – Does not inspect.

Creation of a ZFW using Cisco Common Classification Policy (C3PL)

Create Zones – Create zones using the command 'zone security *name'* command. A 'self' zone is created by default and refers to the router itself. A sub command is available to put a description against the zone. Using SDM, select 'Configure', 'Additional Tasks' followed by 'Zones'. Additionally SDM will allow assigning the zone to an interface at the same time.

Create Zone Pairs – Use the command 'zone-pair security *pairname* source *sourcezonename* destination *destinationzonename'*. A sub command is available to put a description against the zonepair and assign a policy 'service-policy type inspect *policyname'*. SDM 'Configure', 'Additional Tasks' followed by 'Zone Pairs' allows editing, creation & assigning a policy.

Create Class Maps – Used to identify traffic. SDM 'Configure', 'Additional Tasks', 'C3PL', 'Class Map' followed by 'Inspection'.

Create Policy Maps – A policy map defines what action to perform on traffic. Each policy map has one or more class maps assigned together with an action for that traffic. SDM 'Configure', 'Additional Tasks', 'C3PL', 'Policy Map' followed by 'Protocol Inspection'.

Assign interfaces to Zones – Use the 'zone-member security *name'* command under an interface.

C3PL/MQC (Modular QoS CLI) – Parameter maps

Used to create additional parameters to match on. Example-

```
(config) # parameter-map type protocol-info aol-servers          - Create a parameter map for AOL servers
(config-profile) # server name login.oscar.aol.com
(config-profile) # server name toc.oscar.aol.com
(config-profile) # server name oam-d09a.blue.aol.com
```

C3PL/MQC (Modular QoS CLI) – Class maps

Class maps are used to identify and classify traffic. A Class map can match on among others-

- ACLs
- Protocol / NBAR (Network based application recognition). This looks at the packet data to attempt to identify the protocol used e.g. HTTP on a non standard port.
- Another subordinate class map

Two types of inspection class map can be created, a layer 4 map which can match traffic and protocols at layer 4 and Deep Packet Inspection (DPI) class maps which inspect up to layer 7. A DPI map must be nested with in layer 4 class map.

Mode	Description	Command Syntax
(config)	Create a match any class map	Class-map type inspect match-any *name*
(config)	Create a match all class map	Class-map type inspect match-all *name*
(config)	Create a DPI class map	Class-map type inspect protocol match-any name
(config-cmap)	Set match criteria on an ACL	Match access-group *aclno*
(config-cmap)	Set match criteria on input interface	Match input-interface
(config-cmap)	Match based on NBAR	Match protocol *protocol*
(config-cmap)	Match on NBAR with parameter map	Match protocol *protocol parametermap*

NOTE-

- Match-any signifies an or condition between statements
- Match-all signified an AND condition between statements

Examples-

```
(config) # class-map type inspect match-all HTTPFOMACL                - Create map to identify HTTP and ACL 100
(config-cmap) # match protocol http
(config-cmap) # match access-group 100

(config) # class-map type inspect match-any sdm-cls-protocol-im       - Create map to identify IM using NBAR
(config-cmap) # match protocol ymsgr yahoo-servers
(config-cmap) # match protocol msnmsgr msn-servers
(config-cmap) # match protocol aol aol-servers

(config) # class-map type inspect http match-any sdm-http-blockparam- Create map to DPI HTTP
(config-cmap) # match request port-misuse im
(config-cmap) # match request port-misuse p2p
(config-cmap) # match req-resp protocol-violation
```

C3PL/MQC (Modular QoS CLI) – Policy-map

A Policy map controls what to do with traffic identified by a class map.

Mode	Description	Command Syntax
(config)	Create an inpsect policy map	Policy map type inspect *policyname*
(config-pmap)	Add a class map to the policy	Class type inspect *classname*
(config-pmap-c)	Set action for traffic class	Inspect / pass / drop

```
(config) # policy-map type inspect sdm-permit-icmpreply
(config-pmap) # class type inspect sdm-icmp-access
(config-pmap-c) # inspect
(config-pmap-c) # exit
(config-pmap) # class type inspect SDM-Voice
(config-pmap-c) # inspect
(config-pmap-c) # exit
(config-pmap) # class class-default
(config-pmap-c) # pass
(config-pmap-c) # exit
```

IPS

IPS Introduction

Types of IPS/IDS solutions

IDS (Intrusion Detection System) – Sits outside the routing path (Promiscuous mode connected to a SPAN port) and raises alerts in the event of suspicious traffic. This can signal to another router to block traffic but this traffic would have already entered the network, because of this IDSs are vulnerable to "Atomic pattern" attacks where the attack payload is contained in one packet. IDSs are more effective on "Composite pattern" attacks were the attack takes place over multiple packets/hosts.. IDS can get overrun with traffic, as they are not inline traffic flow will not be slowed but malicious traffic could potentially not be checked.

IPS (Intrusion Prevention System) – Sits inside the routing path (Inline mode). As an IPS sits in-line with the traffic flow, the IPS can slow the flow of traffic. In addition to the functionality provided by IDS solutions, an IPS is able to take actions on suspicious traffic-

- Logs (Syslog or SDEE)
- Drops
- Resets the TCP Connection (TCP Reset)
- Blocks the attackers IP address for 'x' minutes. Event action 'Deny Attacker Inline' creates a dynamic access-list to block the IP address.
- Blocks the traffic causing the alarm

HIPS (Host IPS) – A software based IPS on installed on a host.

NIPS (Network IPS) – A router / appliance based IPS. Attackers are now trying to use HTTPS/VPN technologies to bypass detection of a Network based IPS system. Using HIPS on clients would reduce this risk.

Intrusion Detection Methods

Signature – Uses known attacks strings. Low processing requirement but can become out of date if not frequently updated. Zero day attacks will not be detected. Four types of signatures can be used, DoS attack signatures, Exploit signatures to spot byte and traffic patterns of attacks, Connection signatures to identify malicious traffic in an established connection and String signatures which are Regex patterns. Initially signature based analysis can create lots of false positives which signature tuning will reduce/stop.

Policy – Violation of a network policy such as maximum new connections per second (SYN attacks DoS attacks etc), particular IP addresses etc. Policy based methods are able to identify some zero day attacks.

Anomaly – Traffic considered not 'normal'. This requires extensive tuning to avoid false positives. This is sometimes referred to as network behaviour or heuristic analysis.

Honey Pot Detection – An isolated server is placed at risk / not protected in an attempt to draw attacks. IPS will then watch this server to enable better tuning of the IPS system.

Alerts

Bad – False Positive & False Negative. To avoid false positives some signatures may require 'Signature Tuning' or removing a particular signature.

Good – True Positive & True Negative

Signatures

Signature severity levels-

- Informational
- Low
- Medium
- High

Event Actions-

- **Deny Attacker Inline** – Denies the source IP address of the offending packets (Creates dynamic ACL) for a defined period of time.
- **Deny Connection Inline** – Stops the offending packets but not other traffic from the source.
- **Deny Packet Inline** – Drop this packet only.
- **Produce Alert** – Generate an alarm/alert message
- **Reset TCP Connection** – Send a TCP reset to terminate the traffic flow

Cisco IDS / IPS Range

IOS – Some Cisco IOS images implement technology from other IPS/IDS systems to create an IOS IPS.

IDS Network / AIM Modules (AIM-IPS) – Fit inside a router to perform the IDS function taking the load off the routers processor.

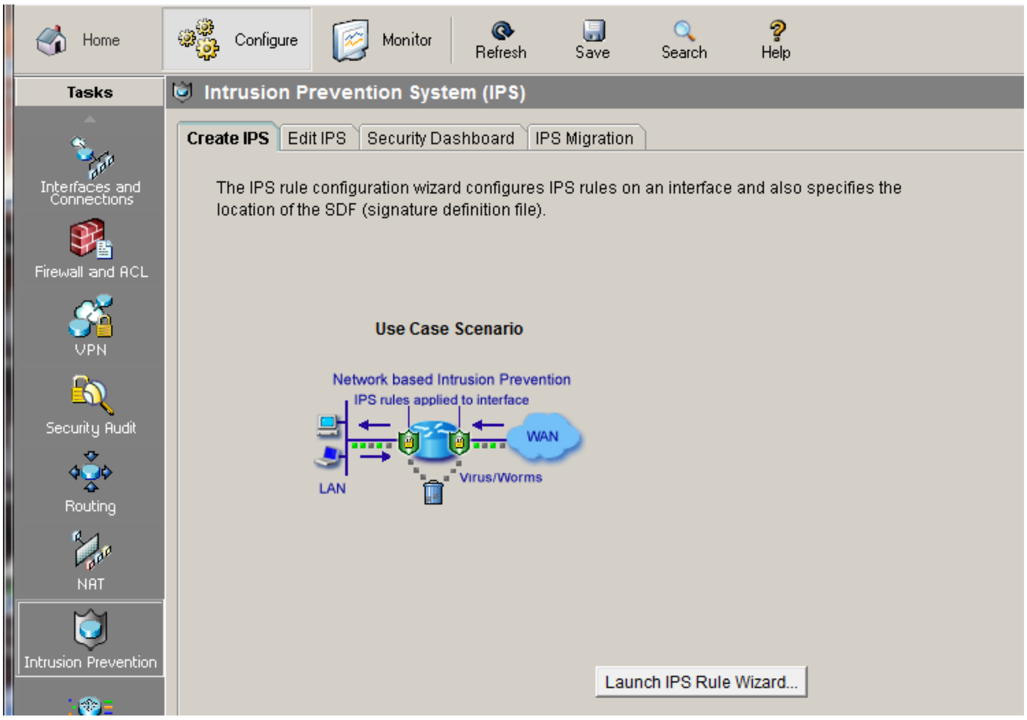
4200 Series Appliances – Dedicated appliance for IPS. Can be run in the routing path or on a SPAN port. The sensors contain at least two interfaces, the command and control interface and the monitoring interface.

Catalyst 6500 IDSM-2 – Fits inside a Cisco 6500 series switches. Able to monitor inter VLAN traffic etc.

Cisco Adaptive Security Appliance Advanced Inspection and Prevention Security Service Module (ASA AIP SSM) – Provides high performance anti-x services.

HIPS (Cisco CSA) – Client software that sits on the end client to identify suspicious traffic on the client. This can capture encrypted attacks which network based solutions cannot detect.

Configuring IPS on a Cisco Router using SDM



The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).

1. Clicking 'Launch IPS Rule Wizard' SDM will enable SSDE on the router and open a subscription with the router so SDM can receive events.

2. The IPS Policy Wizard will now start.

3. Interface selection, set Inbound / Outbound on specific interfaces. Typically IPS will be enabled on the inbound and outbound directions on the internal interfaces, not be on the internet facing connection as this will generate many hundreds of alarms/alerts.

4. Specify the signature file, public key name and key (SDM will not accept IOS-Sxxx-CLI.PKG files on the PC; copy it to flash or tftp/ftp/http and select from there).

5. Choose Config Location. Typically flash:/ or flash:/ips/ on systems which support directories

6. Choose Category – Basic or Advanced (128MB of router memory required).

Configuration generated by SDM-

```
(config) # ip ips notify SDEE                         - Enable SDEE notifications
(config) # ip ips name sdm_ips_rule                   - Define n IPS rule name of sdm_ips_rule
(config) # interface FastEthernet0/0                  - Set which interfaces to enable IPS
(config-if) #  ip ips sdm_ips_rule in
(config-if) #  ip ips sdm_ips_rule out
(config-if) #  exit
(config) # ip ips config location flash:/ips/         - Set the location of the IPS configuration files
(config) # ip ips signature-category                  - Enter the IPS Signature category configuration
(config-ips-category) # category all                  - Select all categories
(config-ips-category-action) # retired true           - Retire all rules
(config-ips-category-action) # exit
(config-ips-category) # category ios_ips advanced     - Select the advanced set of rules
```

(config-ips-category-action) # retired false - Un-retire. The signatures will now be compiled

Edit IPS Tab

IPS Policies – Allows enabling / disabling IPS on individual interfaces and apply an optional ACL to control what traffic is scanned.

Global Settings – Allows setting up the basic IPS properties. Logging. SDEE & Syslog, number of SDEE alerts to store, number of SDDE messages to store and the number of SDEE subscriptions. 'Engine Fail Closed' stops passing packets when the IOS is coming the signatures (disabled by default) 'ip ips failed closed'. Location of the IPS configuration files within the router. Category selection (basic or advanced) and the public key.

Signatures – This displays a category tree of all signatures installed. Each signature can be deleted, enabled/disabled or edited. Typical editable options include severity, alarm interval, event action etc. Once a change is made the modified signature is highlighted in SDM but not directly applied to the router. Click the 'Apply Changes' button to commit the change to the router.

Security Dashboard Tab

The Dashboard allows a user to update the list of top threats from the Cisco IPS Alert Center then deploy the signatures for those threats.

Logging & Monitoring

Reporting / Logging

The outputs of an IDP/IPS system are used to achieve two things, reporting where analysis is performed on historic data and event monitoring to identify when an attack is taking place.

Syslog – Basic reporting method logged to a Syslog server.

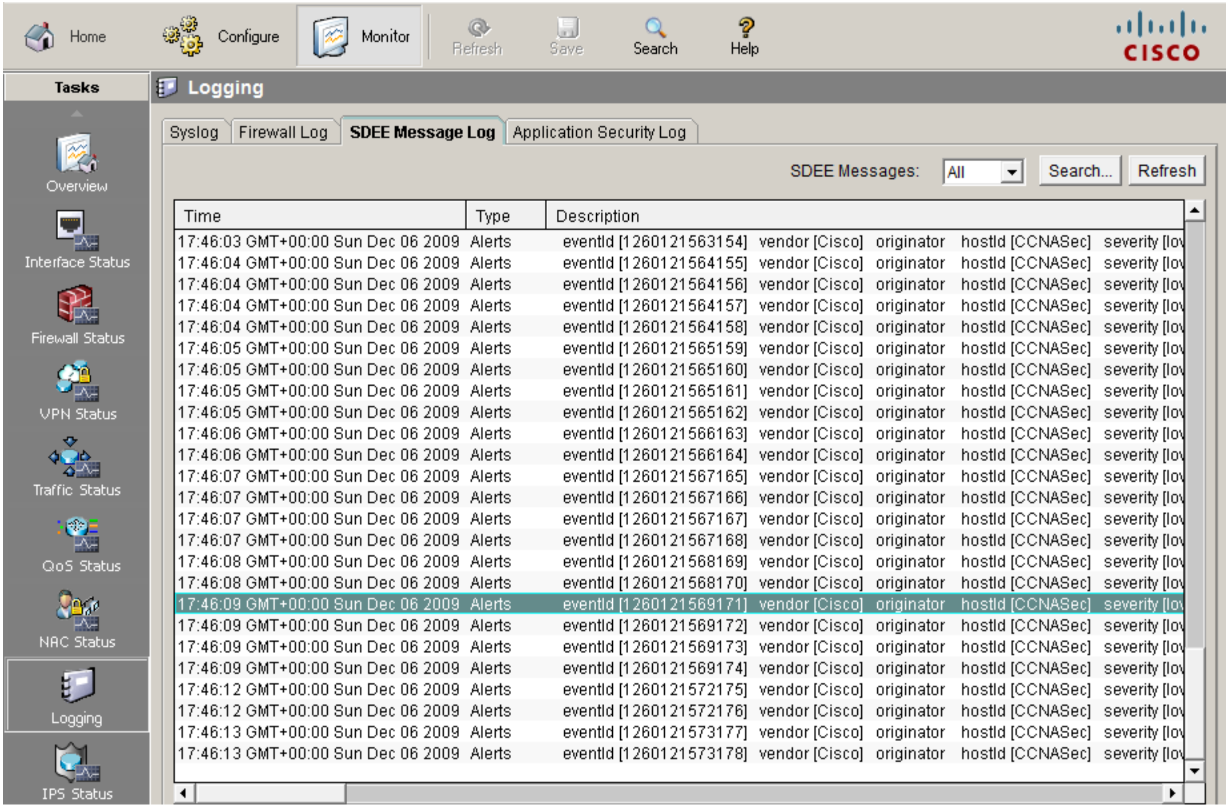
Security Device Event Exchange (SDEE) – Advanced logging method designed specifically for alerting on security devices. SDM can pull these events or the router can be configured to export them to an external server. The router can store up to 1000 (200 by default) events for later retrieval. HTTP/HTTPS must also be enabled to use SDEE.

CLI Monitoring

```
# show ip ips configurations
# show ip ips interfaces
# show ip ips all
```

Monitoring using SDM

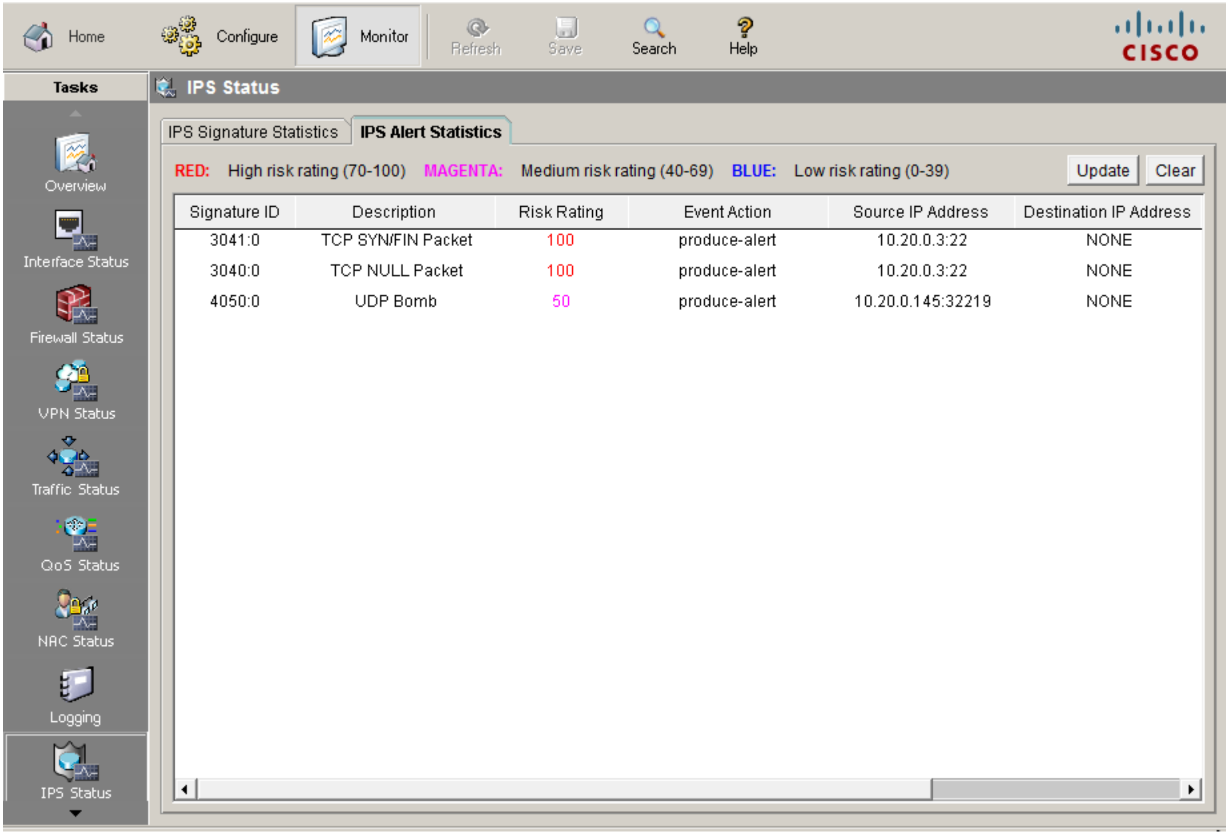
'IPS Status' (shows loaded signatures and hit and drop counts) & 'Logging' followed by 'SDEE Message Log' under the 'Monitoring' section.



Logging

SDEE Messages: All

```
Time                                 Type     Description
17:46:03 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121563154]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:04 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121564155]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:04 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121564156]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:04 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121564157]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:04 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121564158]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:05 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121565159]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:05 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121565160]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:05 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121565161]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:05 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121565162]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:06 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121566163]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:06 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121566164]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:07 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121567165]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:07 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121567166]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:07 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121567167]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:07 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121567168]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:08 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121568169]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:08 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121568170]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:09 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121569171]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:09 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121569172]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:09 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121569173]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:09 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121569174]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:12 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121572175]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:12 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121572176]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:13 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121573177]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
17:46:13 GMT+00:00 Sun Dec 06 2009  Alerts   eventId [1260121573178]  vendor [Cisco]  originator  hostId [CCNASec]  severity [lov
```



IPS Status

RED: High risk rating (70-100) MAGENTA: Medium risk rating (40-69) BLUE: Low risk rating (0-39)

Signature ID	Description	Risk Rating	Event Action	Source IP Address	Destination IP Address
3041:0	TCP SYN/FIN Packet	100	produce-alert	10.20.0.3:22	NONE
3040:0	TCP NULL Packet	100	produce-alert	10.20.0.3:22	NONE
4050:0	UDP Bomb	50	produce-alert	10.20.0.145:32219	NONE

Notes

- VFR (Virtual Fragmentation Reassembly) – Allows the IOS firewall to create dynamic access lists to protect against fragmentation attacks. Helps to protect against Tiny, Overlapping and Buffer Overflow fragment attacks. Command is '*ip virtual-assembly*' under an interface.
- Version 4 IPS definition files consist of Signature Definition Files (SDF) such as '128MB.sdf'.
- Version 5 files are in the format of 'IOS-S360-CLI-pkg' and are singed with a Cisco private key.
- Public Key Name : realm-cisco.pub
- Public Key :

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

VPN / Cryptography

Term	Definition
Cryptology	Science of making and breaking secret codes
Cryptography	Developing and using codes / encryption techniques
Cryptoanalysis	Breaking encryption technologies and codes
Steganography	Technique to hide messages in some other message rather than encrypting the message
Encryption Technologies	
PKCS	Public Key Cryptography Standards – define a set of standards / low level formats for the secure exchange of data
PKCS # 1	RSA Cryptography standard
PKCS # 3	DH Key agreement standard
PKCS # 5	Password based cryptography standard
PKCs # 7	Cryptography message syntax
PKCS # 10	Used for sending certificate requests using SCEP
RSA	Rivest-Shamir-Adelman – SSL,
SSL / TLS	Encryption at the transport layer – Layer 4
IPSec	Encryption at the network layer – Layer 3
V3PN	Voice and Video enabled VPN
DMVPN	Dynamic Multipoint VPN. Allows router to negotiate a point to point VPN with any other router on a hub and spoke VPN topology
X.509	A standard which defines the format for digital certificate transmission and certificate revocation lists (CRL)
Diffie Hellman	Protocol using public / private keys to exchange a shared secret.
Attack Methods	
Brute force	Every possibly key is tried
Cipher text only	The attacker has a number of encrypted message to decrypt
Known plain text	The attacker has both the cipher text and some knowledge of the corresponding plaintext. This can be used in an attempt to derive the key
Chosen plain text	The attacker is able to encrypt some chosen plaintext and vire the cipher text. Improves the chances of deriving the key
Chosen cipher text	Similar to chosen plain text attack
Birthday	Statistically the probability that two people share the same birthday in a group of 23 people is greater than 50%. The same principle can be used when attempting to break a hash function using brute force techniques to improve the chances of breaking the hash
Meet in the middle	The attacker is able to both decrypt cipher text and encrypt plain text in an attempt to find a matching key

Hashing & Digital signatures

Hashing algorithms

- MD5 – 128bit
- SHA-1 – 168bit

A hash function simply calculates a signature/fingerprint/CRC of the message.

HMAC – Hashed Message Authentication Codes

Hashing functions by themselves cannot guarantee the authenticity of the message as anyone can generate a message and calculate a hash. HMAC adds a secret key to the message before applying the hashing routine resulting in a hash that depends on both the message and the key. The receiver of the message can then generate the hash of the plaintext message using the same secret key, if the hash matches then the message is authentic.

Digital Signatures

Digital signatures are similar to the HMAC principle above but use an asymmetric private public key pair. The digest of the message is generated and then encrypted using the private key. The resulting digital signature is attached to the message. The receiver decrypts the digital signature with public key, if the decrypted digest matches the calculated digest of the message the message is authentic and the sender is verified.

Digital Signature Algorithm (DSA) is the current standard for digital signatures.

Symmetric Encryption

The same key is used to encrypt and decrypt. Typically referred to as a shared secret.

Caesar / Substitution Cipher

Characters of a message are substituted with another character from ‘n’ spaces in the alphabet, e.g. ‘a’ becomes ‘m’, ‘b’ becomes ‘n’ etc. Provided the receiving party knows the number of spaces substituted (the key) then encryption is possible. This is very weak as simple character frequency analysis will allow the code to be broken.

Vigenere Cipher

A substitution cipher where the number of characters / spaces moved for each character depends on a corresponding character in a key word, making it invulnerable to a frequency analysis attack. Suppose the phrase ‘ATTACK AT DAWN’ is coded using the key ‘SECRETKEY’, the resulting message will be ‘SXVRGDKXBSAP’.

This uses a table to perform the cipher where the key is on one axis and the message on another to by coded is on the other. Small section below-

	A	B	C
A	A	B	C
B	B	C	D
C	C	D	E

One Time Pad / Vernam Cipher

Uses the principle of a Vigenere cipher but the key is a stream of random characters equal to the length of the message. This results in an almost unbreakable code but with limitations. Creation of a truly random key is almost impossible and it is very difficult to distribute the key. The Vernam Cipher instead XORs the each character of the message with the corresponding key character.

Transposition Cipher

The characters are simply rearranged in the message using a secret sequence. An example is the rail fence cipher

DES (56bit) & 3DES – EDE (112 & 156bit)

4 weak keys, 12 semi weak keys

DES offers two types of ciphers-

- Block Cipher – Electronic Code Book (ECB) and Cipher Block Chaining (CBC). Each 64bit block is encrypted using the 56 bit key.
- Stream Cipher – Output Feedback (OFB) and Cipher Feedback (CFB) modes.

CBC is used by. All but EBC use XOR operations on the previous cipher text block to generate the next cipher block. This avoids the scenario where two identical plaintext packets result in the same cipher text.

3DES Uses three 56bit keys. The message if encrypted wit h the first key, decrypted with the second key then finally encrypted with the third key to derive the cipher text. If the first and third keys are then same then the effective key length is reduced to 112 bits.

AES (128, 192 & 256bit)

Rijndael cipher is an iterated Block Cipher where multiple operations are performed on each block to derive the cipher text.

IDEA (128bit) International Data Encryption Algorithm

Block Cipher

SEAL – Software Encryption Algorithm

A software based stream cipher designed to have a low impact on CPU resources..

RC

RC2 (40 & 56bit) – Stream Cipher
RC4 (1 to 256bit) – A encryption method based on the Vernam cipher, used in SSL & WEP.
RC5 (0 to 2040bit) – A fast block based cipher.
RC6 (126, 192 & 256bit)

Blowfish (32 to 448bit)

Block Cipher

Asymmetric Encryption

A key pair is required, one to encrypt and another to decrypt. Up 100 times slower than symmetric encryption in software and up to 1000 times in hardware.

RSA

RSA named after the inventors (Ron Rivest, Adi Shamir & Leonard Adleman) is a public key infrastructure (KPI) system capable of both encryption and signed requirements. Bock Cipher.

The bit lengths are not directly comparable to symmetric bit lengths. A 1024 bit RSA key is considered equal to an 80 bit symmetric key, 2048 to a 112 bit symmetric key and 3072 to a 128 bit symmetric key.

RSA Vulnerabilities

- **Timing attack** – An attacker could measure the decryption times for a number of cipher texts and if the hardware is known the decryption key could be deduced quickly. Most RSA implementations use a scheme known as blinding to stop the decryption time being correlated to the cipher text.
- **Adaptive chosen cipher text attack** – Uses weaknesses in RSA / PKCS #1 when used in SSL protocols and is used to recovery session keys. An updated version of PKCS #1 has been released which is not vulnerable to this attack.
- **Branch Prediction Analysis attack** – Used in modern processors that use branch prediction and Simultaneous multithreading (SMT). An attack uses a spy process to statistically discover the private key when being processed using these processors.

Diffie Hellman Key exchange

The DH process works by both parties agreeing on two non secret numbers and each party generating a secret number. Each party then generates a public number from its secret and the two non secret numbers and this is passed to the other party. Each party then generates a shared secret by from its own secret and the public number generated on the other party.

1. The two parties agree on two non secret numbers (generator and base). p=23 and base g=5.
2. Party 1 chooses a secret integer a=**6**, then sends Party 2 A = g^a mod p
   - A = 5^6 mod 23 = 8.
3. Party 2 chooses a secret integer b=**15**, then sends Party 1 B = g^b mod p
   - B = 5^{15} mod 23 = 19.
4. Party 1 computes **s** = B^a mod p
   - 19^6 mod 23 = **2**.
5. Party 2 computes **s** = A^b mod p
   - 8^{15} mod 23 = **2**.

Choosing an encryption method

Two main criteria-

1. Does the cryptographic community trust the algorithm
2. Resistance level to brute force attacks

DES, 3DES, IDEA, RC4, AES, RSA and DH are considered trust worthy.

Key Management

- Key Generation – Typically generated using a random number generator.
- Key verification – make sure the chosen key is no 'weak'.
- Key Storage – Storage of the keys in a manner which is considered secure.
- Key Exchange – Ensure any keys exchanges are performed securely.
- Key Revocation and Destruction – A method to notify all interested parties that a key has been compromised ad should not be user.

PKI

PKI uses asymmetric encryption.

Message Confidentiality – the Message is encrypted with the receiving party's public key. Only the receiving party can decrypt the message with their private key.

Message authenticity – The message is encrypted using the senders private key. The message can only be decrypted with the senders public key proving the message is authentic.

A public key infrastructure contains the following parts-

- Certificate Authorities
- Users, people, devices etc
- Storage and Protocols
- Supporting organisational framework
- Supporting legal framework

Certificates

A Certificate contains-

1. Public key of the router.
2. Device signature (name) encrypted with the private key. This can only be decrypted using the public key, proves the router is who he says he is.
3. CA Signature. This is the name of the CA encrypted with the CA private key. Only the CA public key can decrypt the signature proving the certificate was signed by the certification authority.

A certificate can have a certificate class to indicate the trustworthiness of the certificate. Typically a number, the higher the number the more trustworthy the certificate. The higher the class the more must be done to prove the authenticity of the requester. Class 0 may require no checks, class 1 may require an email from the domain to prove identity.

SCEP (Simple Certificate Enrolment Protocol) – Automated method to send certificates to hosts/routers. A host will request a certificate from the CA. Operates in two modes-

Manual – Administrator approves the request

Pre-shared key – Devices will pass a key to the CA to allow the CA to automatically generate the certificate.

Certificate Authority

A trusted third party which sings the public keys. There are multiple topologies for a PKI system-

- Single root – Difficult to scale and vulnerable in that if the root key is compromised all certificates generated are invalid.
- Hierarchical – A root CA in turn issues certificates to subordinate CA's. The subordinate CA's then issue certificates to end users. This improves scalability and reduces the impact if a key is compromised.
- Cross-certifying – A CA will cross certify with another CA on different PKI installation, in effect creating a trust relationship.

A CA perform many tasks in addition to signing user certificates such as authenticating users when they enrol with the PKI, key generation and distribution of certificates. These tasks can be offloaded to a Registration Authority (RA) enabling the CA to concentrate on signing.

Cisco routers support the following appliances / servers -

Entrust
Baltimore
Verisign
Windows 2000

IPSec

Components

Name	Use	Bits	
AH	Protocol	-	Provides Authentication, Data Integrity and Anti replay using HMAC codes. The entire IP Packet is hashed so will not work through NAT
ESP		-	Provides Encryption, Authentication, Data Integrity and Anti replay.
DES (S)	Encryption	56	64 bit keys 8 bits are parity
3DES (S)		168	Three 56 bits keys are used. Key 1 encrypt, 2 decrypt 3 encrypt
AES (S)		128,192,256	
MD5	Hash / Auth	128	
SHA-1		160	
DH1 (A)	Protection	768	VPN Phase 1 initiation, used to create a shared secret key without actually passing the key between two parties.
DH2 (A)		1024	
DH5 (A)		1536	
DH7 (A)			
RSA (A)	Encryption	360 to 2048	SSH,

IPSec Benefits

- Authentication – Ensures the connection is made with the corre3ct remote endpoint.
- Data Integrity – Hashing (HMAC-MD5, HMAC-SHA-1)
- Confidentiality – Data is encrypted as it flows through the VPN
- Anti-Relay – Ensures each packet is unique. Stops man in the middle devices replaying packets in an attempt to cause system issues.

Operation methods

Transport Mode

Data	*ESP*	IP	MAC

Typically used internally (LAN/WAN) to secure inter host communication.

Tunnel Mode

Data	*IP*	*ESP*	IP	MAC

Typically used to secure and tunnel data over the internet.

NOTE – Italics indicate encrypted data

Negotiation

1. Interesting traffic initiates the raising the VPN. Uses an ACL to match interesting traffic.
2. IKE Phase 1. IKEMPE Tunnel.
3. IKE Phase 2. IPSec Tunnel
4. Data is transferred
5. VPN is torn down.

Phase one

Main Mode – Three exchanges-

1. Exchange and negotiate policy and algorithms..
2. Exchange DH keys.
3. Identity verification / authenticates an Internet Security Association and Kay Management Protocol (ISAKMP) session using PSK or certificates.

Aggressive Mode – A total of three packets are sent-

1. The initiator sends all data required to initiate an SA. This data is sent unencrypted
2. The responder replies with the proposal, key, ID and authenticates the session.
3. The initiator replies by authenticating the session.

The result of these transfers is a bi-directional tunnel ready for phase two negotiation.

Phase two

This uses a mode called 'Quick Mode' to negotiate IPSec parameters/transform sets, establish the IPSec SAs, periodically renegotiation the SAs to improve security.

There are two directional IPSec SA's generated during phase 2.

IPSec Authentication

Username / Password – Used for user access VPNs

One time password – Used for user access VPNs

Pre shared key – Typically used for site to site VPNs, both ends have the same pre shared key. Works well for small networks but can become unmanageable for large networks (10 to 15 sites) as ideally the pre shared key should be changed frequently.

Certificates – Each end point receives a certificate from a trusted certificate authority, other endpoints can then verify the endpoint by examining the certificate

1. All routers will enrol with a CA (OOB). This allows the router to trust the CA. The router will receive the CAs public key and certificate to verify the CA.
2. The CA will issue each router with its own certificate.
3. A router can authenticate another router by passing its certificate and public key. The router will decrypt the certificate using the routers public key and verify the CA signature using the CA public key.
4. The routers will then generate a session key (AES, DES etc).

Configuring Site to Site VPNs

Configuring Site to Site VPNs using SDM

SDM Site-to-Site VPN offers two creation modes-

Quick Setup – This uses a number of defaults options. Prompts for the ext interface, interface where the encrypted traffic originates, remote peer IP address, remote destination IP address range and authentication (PSK or certificates). The following defaults are used - Phase 1 : 3DES, SHA_1, DH2. Phase 2 : ESP_3DES, ESP_SHA_HMAC.

Step by Step wizard – Allows defining all parameters. Typical generated config-

```
(config) # access-list 100 remark SDM_ACL Category=4
(config) # access-list 100 remark IPSec Rule
(config) # access-list 100 permit ip 10.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255

(config) # crypto ipsec transform-set VSPTSET esp-sha-hmac esp-3des
(cfg-crypto-trans) # mode tunnel
(cfg-crypto-trans) # exit

(config) # crypto map SDM_CMAP_1  1 ipsec-isakmp
(config-crypto-map) # description Tunnel to4.2.2.2
(config-crypto-map) # set transform-set VSPTSET
(config-crypto-map) # set peer 4.2.2.2
(config-crypto-map) # match address 100
(config-crypto-map) # exit

(config) # interface Vlan1
(config-if) # crypto map SDM_CMAP_1
(config-if) # exit

(config) # crypto isakmp policy 1
(config-isakmp) # authentication pre-share
(config-isakmp) # encr  3des
(config-isakmp) # hash sha
(config-isakmp) # group 2
(config-isakmp) # lifetime 86400
(config-isakmp) # exit

(config) # crypto isakmp key ***** address 4.2.2.2
```

Configuring Site to Site VPNs using CLI

Allow IPSec traffic through the external interface ACLs

- ISAKMP – UDP 500
- ESP – IP Protocol 50
- AH – IP Protocol 51

```
access-list 101 permit udp host 82.70.0.213 host 82.70.0.209 eq non500-isakmp
access-list 101 permit udp host 82.70.0.213 host 82.70.0.209 eq isakmp
access-list 101 permit esp host 82.70.0.213 host 82.70.0.209
access-list 101 permit ahp host 82.70.0.213 host 82.70.0.209
```

ISAKPM Phase 1

Mode	Description	Command Syntax
#	Enable ISAKMP debuging	Debug crypto isakmp
#	Show defines ISAKMP Policies	show crypto isakmp policy
#	Show active ISAKMO Security Associations	show crypto isakmp sa
(config)	Enable ISAKMP globally	Crypto isakmp enable
(config)	Define a isakmp policy	Crypto isakmp policy *no*
(config-isakmp)	Set authentication method	Authentication <pre-share / rsa-encr / rsa-sig>
(config-isakmp)	Set DES / 3DES encryption	Encryption <des / 3des>
(config-isakmp)	Set AES encryption and key length	Encryption aes <128 / 192 / 256>
(config-isakmp)	Set hashing	Hash <md5 / sha>
(config-isakmp)	Set DH group	Group <1 / 2 / 5 / 14 / 15 / 16>
(config-isakmp)	Set the lifetime	Lifetime *seconds*
Set the identity of this router		
(config)	Set method of identifying phase 1 tunnel	crypto identity <address / dn / hostname>
Set the Phase 1 Key for a peer		
(config)	Configure the key for the remote ipaddress	Crypto isakmp key *key* address *ipaddress*
(config)	Configure the key for the remote hostname	Crypto isakmp key *key* address *hostname*

Example-

```
(config) # crypto isakmp enable
(config-isakmp) # crypto isakmp policy 20
(config-isakmp) # authentication pre-share
(config-isakmp) # encryption aes 128
(config-isakmp) # group 2
(config-isakmp) # hash sha
(config-isakmp) # lifetime 28800
(config-isakmp) # exit
(config) # crypto isakmp identity address
(config) # crypto isakmp key VPN address 10.20.0.2
```

IPSec Phase 2

Mode	Description	Command Syntax
#	Debug the IPSec processes	Debug crypto ipsec
#	Show all defines transform sets	show crypto ipsec transform-set

#	Show all crypto maps	show crypto map
#	Show active IPSes SAs	show crypto ipsec sa
#		show crypto engine connections active
#		show crypto session
Create a Transform Set		
(config)	Create a transform set	Crypto ipsec transform-set *tag* <encrypt> <hash>
(cfg-crypto-trans)	Set Tunnelling mode	Mode <tunnel / transport>
Set lifetimes		
(config)	Set IPSec tunnel timeout	Crypto ipsec security-association lifetime seconds *sec*
(config)	Set IPSec lifetime	Crypto ipsec security-association lifetime kilobytes *kb*
Define Crypto map and match ACL		
(config)	Create access list to match traffic	Access-list *no* permit ip x.x.x.x y.y.y.y x.x.x.x y.y.y.y
(config)	Create the map	Crypto map *tag sequence* ipsec-isakmp
(config-crypto-map)	Set the IP addresses to encrypt	Match address *aclno*
(config-crypto-map)	Set remote IP address	Set peer remoteipaddress
(config-crypto-map)	Set the IPSec transform set	Set transform-set *tranformsettag*
Apply the Crypto map to an interface		
(config-if)		Crypto map *maptag*

NOTE – only one crypto map tag can be assigned to an interface but multiple crypto maps can be configured against the tag be using different sequence numbers.

```
(config) # crypto ipsec transform-set VPNTRANSFORM esp-aes 128 esp-sha-hmac
(cfg-crypto-trans) # exit

(config) # crypto ipsec security-association lifetime seconds 3660
(config) # access-list 150 permit ip  172.31.1.0 0.0.0.255  172.31.0.0 0.0.0.255
(config) # crypto map VPN 1 ipsec-isakmp
(config-crypto-map) # match address 150
(config-crypto-map) # set peer 10.20.0.2
(config-crypto-map) # set transform-set VPNTRANSFORM
(config-crypto-map) # exit

(config) # interface fastethernet 0/0
(config-if) # crypto map VPN
(config-if) # exit

(config) # ip route 172.31.0.0 255.255.255.0 10.20.0.2
```

Clear a Tunnel

```
# clear crypto isakmp
# clear crypto sa
```

Endpoint Security

Endpoint Security Introduction

Operating Systems

Operating systems provide some basic security services to applications-

- **Trusted Code** – Ensures code / OS system is not compromised using a HMAC (Hash Message Authentication Code) or digital signatures.
- **Trusted Path** – A facility to ensure that a user is performing a genuine operation rather than a Trojan horse. E.g. Ctrl-Alt-Delete to login to a Windows OS.
- **Privileged context of execution** – Provides some identity authentication and privileges based on the identity of the user.
- **Memory isolation** – Protects the memory space of one application from others.
- **Access control** – Restrict access to files from unauthorised users.

Additionally other techniques can help protect endpoints-

- **Least privilege** – A process/user should never be given higher privileges than required.
- **Isolation between processes** – An OS should isolate a process from mall other processes.
- **Reference Monitor** - A control concept that provides a mechanism then mediates all access to objects
- **Small verifiable pieces of code** – Small code blocks that do a small amount of work in a controlled, bug free and secure manner. These can be monitored by the reference monitor

Applications

Application attacks are one of two types-

- **Direct** – An attacker get the application to perform a task.
- **Indirect** – An attacker compromises a different system and then launches an attack to the target through the compromised system (privilege escalation)

Phases of an attack

- **Probe** – Find vulnerable targets using ping sweeps, open ports scans etc.
- **Penetrate** – Once a vulnerable system is found, take advantage of the vulnerability to gain access to the system..
- **Persist** – Once the vulnerable code is on the target and running, find a way of ensuring the code runs at all times even after a reboot.
- **Propagate** – Find other vulnerable systems in order to spread the attack to other systems.
- **Paralyse** – Carry out the malicious action (erase data, steal data, cause DoS, launch a distributes DoS attack etc).

Example of some previous attacks and their phases

Phase	Morris (198)	Log Bug (2000)	Code Red (2001)	Slammer (2003)	MyDoom (2004)	Zolob (2005)
Probe	Scan for fingerd	-	Scan for IIS	-	-	Scan for MS Directory Services
Penetrate	Buffer overflow in fingerd	Email attachment	Buffer overflow in IIS	Buffer overflow in MSDE and MSSQL	Email attachment	Buffer overflow in UPnP
Persist	Execute script to download code	Create executable and edit registry	Execute script to download code	-	Create executable and edit registry	Create executable, edit the registry and download code
Propagate	Look for email address to spread	Open address book and email copies	Pick new address and spread to new victims	Pick new address and spread to new victim	Open address book and email copies	Start FTP and FTFTP services
Paralyse	Run many process to slow the system	Worm spreads	Run many process to slow the system	Generate lots of network packets to slow network	Worm spreads	Delete registry keys, files and terminate processes

Cisco NAC

NAC is designed to only allow authorised and compliant systems access to the network by providing four main features-

- Authentication and authorisation
- Posture assessment – Evaluates the security of the device against defines policies
- Quarantining of noncompliant systems
- Remediation of noncompliant systems

NAC Components

NAC Framework – A framework using the Cisco network infrastructure and third-party systems using software modules embedded within NAC enabled devices.

Cisco NAC Appliance – A self contained appliance that performs all the NAC functions. Does not require Cisco infrastructure.

Cisco NAC Appliance Server (NAS) – A device that perms network access control and device compliance checks as users access the network.

Cisco NAC Appliance Manager (NAM) – A centralised web based administrative tool for managing users and security policies.

Cisco NAC Appliance Agent – Software that runs on the client / endpoint computer that is used to audit the endpoint to compliance and launch updates.

The NAC Process

1. The user attempt to access a network resource
2. User is redirected to a login page.
3. The host is scanned for posture compliance.
   a. It not compliant the host if quarantined to a separate VLAN which only allows the host to be patched / remediated
   b. If complaints the host is granted access to the network.

Cisco Security Agent (CSA)

A hot based security solution designed to prevent s host being compromised by DoS, Worms, Spyware, Viruses etc. CSA is not a conventional signature based virus/spyware scanner but functions as a host based IPS (HIPS) to detect anomalies or signs of undesirable behaviour such as Windows registry changing, launching port scans etc. CSA operates by intercepting operating system and application calls using four interceptors which examining the calls against security policies. If a policy of violated an error message is passed back to the calling application and an alert is generated to be sent to the Management Centre for CSA. The interceptors combines give the following functionality, distributed firewall, HIPS, Application sandbox, network worm prevention and file integrity monitoring.
Interceptors-

- **File system Interceptor** – Scans all file read and writes.
- **Network Interceptor** – All network access is scanned. This also can limit the number of network connections allowed within a specific time to prevent DoS attacks.
- **Configuration Interceptor** – Read and write attempts to the registry in Windows and rc files in Unix systems checked for compliance.
- **Execution Space Interceptor** – Detects and blocks attempts to access memory not owned by the calling application

The agent runs in two modes.

- Headless – The agent is installed in a standalone configuration.
- Managed – The agent is managed by and reports to Cisco CSA Management Centre and/or MARS.

IronPort

Cisco IronPort security appliances protect networks from internet based threats, particularly email and web security. The range consists of three products-

- **IronPort C-Series** – Email security. The basis of the email security appliance is SenderBase (http://www.senderbase.org) which collects date from more than 100,000 ISP and other organisations on various email parameters derive trends and virus/spyware propagation data. This appliance implements a full mail transfer agent and can provide anti-x capabilities, policy enforcement and mail routing.
- **IronPort S-Series** – Web security using Web Reputation data (trustworthiness) and a Dynamic Vectoring and Streaming (DVS) engine to provide signature based spyware filtering
- **IronPort M-Series** – Management, reporting and spam quarantine management

San and Voice Security

SAN Security

SANs help reduce capital and operating expenses, increase storage versatility to respond to changing business priorities & requirements and improve backup, replication & recovery.

Communication types-

- **Fibre Channel** – The primary SAN transport for host to SAN communications.
- **iSCSI** – This uses an IP network to transport the SCSI communications between a host and a storage system. This is cheaper to implement as the existing network infrastructure can be used.
- **FCIP** – Used to connect SAN to SANs over an IP network (WAM or MAN)

Logical Unit Number (LUN) – An address for an individual disk/volume on SCSI bus / HBA.

World Wide Name – A 64bit address used by Fibre Channel networks to identify each element. This is written like 54:25:B5:3E:76:FE:43:FF.

Host Bus Adaptor (HBA) – the interface card that is installed in a server to communicate with the fibre channel infrastructure

Securing SANs

- LUN Masking – An authorisation process than allows access to a LUN at the host bus adaptor level. This on not considered secure as the HBA could become compromised or the source address could be forged. This is typically used as a means to stop misbehaving servers from corrupting disks not belonging to themselves.
- Soft zoning – This partitions the SAN into smaller subsets by restricting the name services in the fibre channel fabric/switches from advertising the devices a host is not allowed to communicate with. Is the host already knows the volume address it can still gain access.
- Hard zoning – This restricts access using ACLs applied to the fibre channel switch port ASICs.
- Virtual SAN (VSAN) – Similar to network VLANs.

Port Authentication

Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) – Password based key exchange protocol supporting switch to switch and host to switch authentication.

Challenge Handshake Authentication Protocol (CHAP) – The mandatory protocol using shared secrets for iSCSI authentication.

Fibre Channel Authentication Protocol (FCAP) – This uses certificates (or keys) to authenticate hosts. It requires a PKI and has such has strong security capabilities. The only significant disadvantage is the requirement of a PKI.

Fibre Channel Password Authentication Protocol (FCPAP) – Optional password based authentication key exchange protocol offering mutual authentication between fibre channel ports. This has many of the benefits of FCAP without requiring a PKI.

Data Confidentiality

Two protocols are available to ensure data confidentiality when in transit-

- ESP
- Fibre Channel Security Protocol (FC-SP)

Voice Security

Definitions-

- **VoIP** – Transmission of voice data over an IP network.
- **IP Telephony** – Is the superset of VoIP including all telephony aspects such as dialling, signalling, gateways, gatekeepers, QoS etc.
- **Gatekeeper** – AKA Cisco Multimedia Conference Manager (MCM) provides bandwidth management, call admission control, address translation.
- **Gateway** – Translation between IP and traditional telephony (PSTN, Fax machines, PBXs)
- **Call Agent** – Provides call control. CUCME & CUCM function as call agents.
- **Some benefits of VoIP** – Cost savings, flexibility, advanced features (advanced call routing, unified messaging, long distance toll bypass, encryption).

Voice Attacks-

SPIT – Span over IP telephony.

Vishing – An attacker attempts to gain confidential information over a telephone.

Toll Fraud – Inappropriate use of a telephony system to make long distance / international calls.

SIP Attacks – Use the open SIP standard to intercept or manipulate SIP messages or launch a DoS attack.

Eavesdropping – Listening on conversations.

Approaches to secure VoIP

Auxiliary / Voice VLANs – Use auxiliary VLANs when daisy chaining PCs to the Phones switch ports. The PC will not be able to access the phones RTP stream

Encapsulation/VPN – The SCCP (Skinny) communications between a phone and CUCM can be encapsulated into TLS/SSL. Additionally the RTP stream between phones can be secured using TLS/SSL (SRTP).

Phone loads/Images – Loads can be signed using a Cisco private key to ensure only Cisco phone images are loaded on to a phone.

Phone configuration files – Can be signed with a private key of the TFTP server to ensure the config files are genuine. In effect the phone will only accept config files from the specified TFTP server.

IP Phone vulnerabilities

Cisco IP phones by default have a unsecured web interface accessible using HTTP. Web access and other vulnerabilities such as Gratuitous ARP can be disabled on the CUCM ephone configuration screens.

Notes

Open DNS server 4.2.2.2

Syslog Server - Kiwi Syslog Server http://www.kiwisyslog.com/

SNMP Logging Toot - http://www.splunk.com/product

Vulnerability Scanner - http://www.nessus.org/nessus/