

# CCNA Security

## (640-553)

 Smarter  
Training

LearnSmart's CCNA Security exam manual helps network professionals prepare for the 640-553 exam by presenting complex topics as clearly and directly as possible. By studying this guide, candidates will become familiar with numerous CISCO security concepts found in the exam, including:

- Security threats
- Securing CISCO routers
- Implementing AAA and Cisco routers
- Mitigating threats to Cisco routers and networks
- And more!

Give yourself the competitive edge necessary to further your career as a network professional and purchase this exam manual today!

# CCNA Security (640-533 IINS)

## LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC.

Product ID: 012203

Production Date: July 6, 2011

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

### Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

### Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

**1-800-418-6789**

[solutions@learnsmartsystems.com](mailto:solutions@learnsmartsystems.com)

### International Contact Information

**International:** +1 (813) 769-0920

**United Kingdom:** (0) 20 8816 8036

<b>Domain 1 - Describe the security threats facing modern network infrastructures</b>	<b>7</b>
Basics	7
Classification	7
<i>Government and Military Model</i>	7
<i>Organizational Model</i>	7
<i>Roles</i>	8
Security Controls	8
<i>Control Classification</i>	8
Law	8
Attack Categories	9
IP Spoofing Attacks	9
<i>IP Source Routing</i>	9
<i>Prevention</i>	9
Confidentiality Attacks	10
Integrity Attacks	10
Availability Attacks	11
System Development Life Cycle (SDLC)	11
Backup Sites	12
Security Policy	13
<i>Security Policy Components</i>	13
<i>Risk Analysis</i>	14
<i>Risk Mitigation</i>	14
Security Awareness	14
Cisco Self-Defending Network	15
<i>Core Characteristics</i>	15
Cisco Integrated Security Products	15
<b>Domain 2 - Secure Cisco routers</b>	<b>15</b>
Security Device Manager (SDM)	15
<i>Security Audit</i>	16
Securing Passwords	17
<i>Enable Password</i>	17
<i>Enable Secret Password</i>	18
<i>Line Passwords</i>	18
<i>Local User Passwords</i>	18

<i>Password Recovery</i> .....	18
<i>Configuring Cisco Password Encryption</i> .....	19
<i>Configuring Miscellaneous Password Parameters</i> .....	19
Privilege Levels .....	19
Role-Based CLI .....	20
Securing IOS Images and Configuration Files .....	20
<b>Domain 3 - Implement AAA on Cisco routers</b>	
<b>using local router database and external ACS</b> .....	<b>21</b>
Authentication, Authorization and Accounting (AAA) .....	21
AAA Configuration .....	21
<i>Authorization</i> .....	24
<i>Accounting</i> .....	26
<i>AAA Debug</i> .....	27
SDM AAA Configuration .....	27
TACACS+ and RADIUS .....	31
<i>TACACS+ Responses</i> .....	31
<i>TACACS+ Attributes</i> .....	31
<i>RADIUS Message Types</i> .....	31
<i>RADIUS Attributes</i> .....	32
AAA Server Configuration .....	32
<i>TACACS+ Configuration</i> .....	32
<i>RADIUS Configuration</i> .....	32
<i>SDM TACACS+/RADIUS Server Configuration</i> .....	33
Cisco Secure ACS .....	34
<i>Cisco Secure ACS Requirements</i> .....	34
<i>Cisco Secure ACS Connections</i> .....	35
<b>Domain 4 - Mitigate threats to Cisco routers and networks using ACLs</b> .....	<b>35</b>
Access Lists Types .....	35
Access List Configuration .....	35
<i>SDM Access-list Configuration</i> .....	38
Access List Caveats .....	40
Preventing IP Spoofing .....	40
<b>Domain 5 - Implement secure network management and reporting</b> .....	<b>41</b>
Secure Management and Reporting Planning .....	41

Secure Management Architecture .....	41
Secure Shell .....	41
<i>Configuring Secure Shell</i> .....	42
<i>Configuring SSH with SDM</i> .....	43
Syslog .....	46
<i>Configuring Syslog</i> .....	47
<i>Configuring Syslog with SDM</i> .....	47
Simple Network Management Protocol (SNMP) .....	48
<i>SNMP Components</i> .....	48
<i>SNMP Message Types</i> .....	49
<i>SNMP Security Levels</i> .....	49
<i>Configuring SNMP</i> .....	49
<i>Configuring SNMP with SDM</i> .....	50
Network Time Protocol (NTP) .....	51
<i>Configuring NTP</i> .....	51
<i>Configuring NTP with SDM</i> .....	52
<b>Domain 6 - Mitigate common Layer 2 attacks .....</b>	<b>52</b>
VLAN Hopping .....	52
Configuring VLAN Hopping prevention .....	52
<i>Switch Spoofing</i> .....	52
<i>Double Tagging</i> .....	53
Root Guard .....	53
Configuring Root Guard .....	53
Portfast .....	53
Configuring Portfast .....	54
BPDUGuard .....	54
Configuring BPDUGuard .....	54
DHCP Snooping .....	54
Configuring DHCP Snooping .....	54
Dynamic ARP Inspection (DAI) .....	55
Configuring DAI .....	55
Port Security .....	55
<i>Port Violation Behaviors</i> .....	55
<i>Secure MAC Address Types</i> .....	56

Configuring Port Security .....	56
<b>Domain 7 - Implement the Cisco IOS firewall feature set using SDM .....</b>	<b>57</b>
<b>Domain 8 - Implement the Cisco IOS IPS feature set using SDM .....</b>	<b>61</b>
<b>Domain 9 - Implement site-to-site VPNs on Cisco Routers using SDM .....</b>	<b>64</b>
<b>Practice Questions .....</b>	<b>67</b>
<b>Answers &amp; Explanations .....</b>	<b>72</b>

# Domain 1 - Describe the security threats facing modern network infrastructures

## Basics

The first thing that must be clear when studying for any security exam is the basics of what network security is about. There are three main goals which are defined to achieve network security:

- Confidentiality – In order to achieve confidentiality, the data being held or transferred is kept private.
- Integrity – In order to achieve integrity, the data must be ensured to be unmodified.
- Availability – In order to achieve availability, data must remain accessible to anyone trying to access it.

## Classification

Organizations can benefit from structuring their own data classification model after pre-existing models. There are two main classification models which are used to classify data:

- Government and Military Model
- Organizational Model

### Government and Military Model

The following classifications are used by both the government and the military. These different classifications include:

- Unclassified – Data which has few or no privacy requirements.
- Sensitive but unclassified – Data which could be embarrassing but is not a security threat.
- Confidential – Data which has a reasonable probability of causing damage if disclosed.
- Secret – Data which has a reasonable probability of causing serious damage if disclosed.
- Top-Secret – Data which has a reasonable probability of causing exceptionally grave damage if disclosed.

### Organizational Model

The following classifications are used by private organizations:

- Public – Data which can be made available.
- Sensitive – Data which could be embarrassing but is not a security threat.
- Private – Data which should be kept secret inside the organization.
- Confidential – Data which is sensitive and should be kept secret inside the organization.

## Roles

Members of an organization assume a number of different roles as they relate to security, including:

- Owner – The owner initially determines the classification levels of the data and reviews the procedures for classifying data. The owner then passes responsibility of data protection to the custodian.
- Custodian – The custodian takes care of the data, including the backup and restoration of data and the verification of data integrity. The custodian is also responsible for following policy in maintaining data.
- User – The user accesses and uses the data per policy guidelines and takes measures to protect the data according to the security policy established by the owner and maintained by the custodian.

## Security Controls

There are a number of controls which can be implemented to maintain a secure solution. These are split into three types, including:

- Administrative Controls – These controls are policy-centric and include clear security policies and good security awareness training.
- Physical Controls – These controls maintain a secure environment and prevent potential physical attacks.
- Technical Controls – These controls include both hardware and software solutions which are implemented to protect data. This is the type of control which is the focus of this exam.

## Control Classification

Each of the three different security control types can be further classified into one of three types:

- Preventive – This type attempts to prevent access to data or systems which contain data.
- Deterrent – This type attempts to prevent data access by influencing a potential attacker from launching the attack.
- Detective – This type attempts to detect when either the data is accessed or when the system containing the data is accessed.

## Law

In most countries legal issues are separated into three major categories, including:

- Criminal Law – Criminal law involves crimes which have been committed that may result in fines and/or imprisonment.
- Civil Law – Civil law involves wrongs which have been committed which are not considered crimes but may involve consequences including paying damages or cease and desist of illegal activity.
- Administrative Law – Administrative law involves the enforcement of regulations by the government agencies.



## Attack Categories

Attacks can be categorized into five broad categories, including:

- **Passive Attacks** – This type of attack happens when the attacker passively listens to traffic and/or tries to decrypt captured packets. These are very hard to detect.
- **Active Attacks** – This type of attack happens when the attacker is actively sending traffic toward the network in an attempt to access unauthorized data. This type of attack is easy to detect.
- **Close-In Attacks** – This type of attack involves an attacker who is physically close to the target data equipment. The attacker can then take advantage of attack types which require physical access.
- **Insider Attacks** – This type of attack involves an attacker who is a legitimate user who tries to access unauthorized data.
- **Distribution Attacks** – This type of attack happens before equipment is distributed and involves the introduction of “back doors” which are taken advantage of once the equipment is at its destination.

## IP Spoofing Attacks

The concept of IP spoofing is simple; it involves the faking of an IP address as being trusted by the target network. Obviously if an attacker is able to make the target system believe that they are coming from a trusted IP then attacks become easier as external attack prevention is circumvented. There are two different types of IP spoofing attacks which include:

- **Nonblind spoofing** – This type is an attack from the same IP subnet as the target, allowing packet capture tools to be used.
- **Blind Spoofing** – This type is an attack not from the same subnet. Often IP source routing is used when performing a blind spoofing attack.

## IP Source Routing

IP source routing allows the attacking machine the ability to specify the exact return path of an IP packet. There are two different types of IP source routing which can be used, including:

- **Loose** – A source route which is loosely followed as the routing equipment can change the path used.
- **Strict** – A source route which is strictly followed by using the exact sequence of hops specified.

## Prevention

There are three main ways used to prevent IP spoofing attacks, including:

- **Access Control Lists (ACL)** – ACLs can be used to prevent internal IP addresses from being used from an external interface. Internal traffic destined for external interfaces should be checked to ensure that the address being used is sourced from an internal IP address range.
- **Link encryption** – The use of link encryption prevents the attacker from capturing and reading packets to obtain useful data.
- **Cryptographic authentication** – If the parties involved in exchanging data are both authenticated to ensure identity, then an attack is highly unlikely.

## Confidentiality Attacks

There are a number of different attack strategies which can be used to affect the confidentiality of data. These include:

- Packet Capture – This is a simple strategy: capture target traffic in order to obtain information that could be used to affect the confidentiality of the target data.
- Ping Sweeps and Port Scans – These techniques can be used to map out a target's network and to figure out what services are being run on these machines. Ping sweeps are used to identify devices and port scans are used to verify active TCP/UDP ports.
- Dumpster Diving – This involves the sifting through of the targets trash in order to find confidential data.
- Electromagnetic Interface Interception – This involves the capture of data by utilizing the EMI which is a side effect on wire media.
- Wiretapping – This involves the capture of data through a physical tap of target wiring systems.
- Social Engineering – This involves the use of non-technical social techniques to obtain confidential data from unknowing individuals.
- Sending Information over Overt Channels – This involves the sending of data over a primary channel but obscured in some way; techniques include tunneling of data and steganography.
- Sending Information over Covert Channels – This involves the sending of data over a secondary non-obvious channel.

## Integrity Attacks

Integrity attacks focus on trying to change the data that is being sent in a way that is not noticed. There are a number of different types of integrity attacks including:

- Salami Attack – A collection of small attacks that result in a larger attack.
- Data Diddling – The process of changing data before it is stored on a computing system.
- Trust Relationship Exploitation – Involves the exploitation of a device which has a trust relationship with the target.
- Password Attacks – Includes a number of different password exploitation attacks including Trojan horse programs, packet capture, keylogger programs, brute force, and dictionary attacks.
- Botnet – Involves the infection of remote machines that become drones or “robots” which can be used to source an attack. These “robots” are controlled remotely and focused on the target.
- Hijacking Sessions – Involves the hijacking of an already initiated user session; this way, the target still believes that the attacker is a legitimate user.

## Availability Attacks

Availability attacks focus on affecting the availability of the target system. There are a number of different attacks which can be used to affect availability including:

- Denial of Service (DoS) – A Denial of Service attack involves the transmission of a large amount of data (flood) and/or requests which is used to consume the resources of the target system.
- Distributed Denial of Service (DDoS) – A Distributed Denial of Service attack involves the same techniques of a normal DoS attack but from multiple sources. These sources are typically compromised systems which are used to direct multiple flows of traffic at the target.
- TCP SYN Flood – A TCP SYN flood involves the attack of a target system by attempting to consume the available TCP sessions on the target device. This is accomplished through beginning but not finalizing a TCP handshake with the target device.
- ICMP Attacks – There are a number of different ways to utilize ICMP in an attack. These attacks are typically DoS in nature.
- Electrical Disturbances – As all computing devices require an electrical source, the effect of many different electrical problems can affect availability. These include spikes, surges, blackouts, and brownouts, among others. These types of attacks can be mitigated through the use of uninterruptable power supplies, power conditioners, and generators.
- Physical Environment Attacks – An environment can also be influenced through the alteration of the physical environment. This includes changes in temperature, humidity and gas. The easiest way to mitigate these types of attack is to control the physical security of the environment.

## System Development Life Cycle (SDLC)

A network as a whole is in constant motion; the different network hardware and software components have a specific lifecycle that should be followed which allows them to have a useful lifetime and to have a point where they are retired. The SDLC describes this cycle with five phases including the following:

- **Initiation**
  - ▶ Security Categorization – Categorizes the severity of a security breach on a specific network component. These devices are typically placed into high, medium and low risk categories.
  - ▶ Preliminary Risk Assessment – Provides a high-level overview of a system's security requirements.
- **Acquisition and Development**
  - ▶ Risk Assessment – Specifies the initial protection requirements.
  - ▶ Security Functional Requirement Analysis – Identifies what is required to properly secure a system so it can function in its intended capacity.
  - ▶ Security Assurance Requirements Analysis – Provides evidence that the network resource in question will be protected at a desired level.
  - ▶ Cost Considerations and Reporting – Details the costs of securing a system.
  - ▶ Security Planning – Details what security controls are to be used.
  - ▶ Security Control Development – Details how the already determined security controls are to be designed, developed, and implemented.
  - ▶ Development Security Test and Evaluation – Validates the operation of the implemented security controls.

- **Implementation**
  - ▶ Inspection and Acceptance – The installation of a system and its functional requirements are verified.
  - ▶ System Integration – The system is integrated with all required components and operation is verified.
  - ▶ Security Certification – The operation of security controls is verified.
  - ▶ Security Accreditation – The system is given administrative privileges to process, store and/or transmit specific data.
- **Operations and Maintenance**
  - ▶ Configuration Management and Control – Before any configuration change is made its impact on other part of the network is analyzed.
  - ▶ Continuous Monitoring – After a security solution is implemented it should be routinely monitored and tested to validate operation.
- **Disposition**
  - ▶ Information Preservation – Any information which is required to be stored should be archived to a modern storage technology to ensure data availability.
  - ▶ Media Sanitation – Storage media that is being disposed of should be sanitized so that the data is not retrievable.
  - ▶ Hardware and Software Disposal – The disposal of both hardware and software should be done through a formal procedure which provides for protection against malicious activities.

## Backup Sites

Backup sites are used to provide redundancy or high availability to critical data. Below are the different types of backup sites used today:

- Hot sites are ready-to-run, dedicated sites that have equipment, software, and real-time data in place. These sites are used to provide highly available data with little to no downtime.
  - ▶ These sites are the most expensive type of disaster recovery arrangement.
  - ▶ They are generally used by organizations in extremely data-sensitive industries, such as financial services, public safety, and healthcare.
- Warm sites provide all of the equipment and environmental controls necessary to restore operations but do not have applications installed or data restored.
  - ▶ These sites take longer to activate than hot sites but are typically much less expensive.
  - ▶ They may be shared by multiple organizations.

- Cold sites are buildings with proper infrastructure to support computing operations (i.e., power, environmental controls, etc.) but without any computer equipment, data, or software in place.
  - These sites are the cheapest alternative.
  - They take a very long time to bring to an operational state.
  - They are useful only in disasters that last for an extended period of time.
- Hot sites, warm sites, and cold sites may be either owned and operated by the organization that they serve, or by a subscription service that keeps the facilities available for its clients.

## Security Policy

The development of a comprehensive security policy is important for the network security of an organization. It is a constantly changing document that sets up guidelines for network use. The main purpose of this policy is to protect corporate assets but it also should be designed to educate users and describe a baseline for security monitoring.

One major part of the security policy is the establishment of an Acceptable Use Policy (AUP). The AUP identifies what users of a network are and are not allowed to do on and with the network.

## Security Policy Components

There are four main components that should be part of the security policy:

- Governing Policy – This is a high-level policy which addresses important security concepts and is primarily targeted at managerial and technical employees.
  - Technical Policies – These policies are used to provide a much higher level of detail of the organization's security policy.
  - End-User Policies – These policies are intended to address security issues and procedures which are relevant to end users.
  - Standards, Guidelines and Procedures:
    - Standards – Define mandatory practices of network use.
    - Guidelines – Define a set of suggested practices of network use.
    - Procedures – Detailed documents which are used to specify step-by-step instructions for the completion of specific tasks.

## Risk Analysis

Risk Analysis is defined as a method of analyzing the probability that a specific threat will occur and the severity of consequences that it brings to the network. There are two different methods for analyzing risk:

- Quantitative analysis – Uses mathematical models to forecast the probability and severity of risk. In the following equations, you are calculating Annualized Loss Expectancy (ALE) and Single Loss Expectancy (SLE) based on the relationships between an asset's value (AV), its exposure factor (EF) and, in the case of the ALE, an Annual Rate of Occurrence (ARO).
  - ▶  $ALE = AV * EF * ARO$
  - ▶  $SLE = AV * EF$ 
    - AV = Asset Value
    - EF = Exposure Factor
    - ARO = Annualized Rate of Occurrence
- Qualitative analysis – Uses behavior models to attempt to predict the probability that someone would want to cause a risk and how much they want to achieve it. This analysis method is more useful when analyzing large networks.

## Risk Mitigation

- Risk Management – Assumes that not all potential threats can be eliminated and attempts to reduce anticipated damage from risk.
- Risk Avoidance – Eliminates identified risks by not exposing a system to end users.

## Security Awareness

User awareness is a big part of the security of a network. In order to make sure that a good security awareness program is implemented, it is recommended that three different core components be fulfilled:

- Awareness – If the end users of the network are aware of the different security threats which exist, they will be more likely to notice when they are happening.
- Training – A good training program creates end user competence and allows them to perform specific tasks and serve in different security roles.
- Education – A more comprehensive education program allows the coverage of a larger amount of material to be covered.

## Cisco Self-Defending Network

The concept behind a self-defending network is simple: have the network try to recognize threats in real time and have it automatically adjust to deal with the specific threat. A part of this concept requires close integration of individual network security products. Cisco's Self-Defending Network is a marketing term that defines a collection of security best-practice solutions which identify threats and attempt to prevent them as well as emerging threats.

### Core Characteristics

There are three core characteristics of the self-defending network:

- Integrated – Security is built into the network instead of being added to an existing network.
- Collaborative – Both IT personnel and security personnel work together on network operations.
- Adaptive – Security solutions are designed to adapt to evolving threats.

## Cisco Integrated Security Products

There are a number of different products that have been introduced by Cisco to provide security solutions. Some of the major products which are currently in use include:

- Cisco Router
- Cisco ASA 5500 Series
- Cisco PIX 500 Series
- Cisco 4200 Series IPS
- Cisco Security Agent
- Cisco Security Access Control Server
- Cisco Catalyst 6500 series switches
- Cisco Router and Security Device Manager (SDM)
- Cisco Security Monitoring, Analysis, and Response System (MARS)

## Domain 2 - Secure Cisco routers Security Device Manager (SDM)

Cisco's Security Device Manager (SDM) provides a way to graphically configure a router through a web interface or through SDM software. This software includes a number of different wizards which can be used to configure the router to perform certain functions without a high level of router knowledge. In order to be able to work with SDM, the router must be installed and configured. There are two ways to use SDM, but both require the same commands to enable its use on the router.

```
router(config)#ip http server  
  
router(config)#ip http secure-server  
  
router(config)#ip http authentication local  
  
router(config)#username name privilege 15 secret password
```

The first two commands are used to enable HTTP access; “secure-sever” enables secure access. A username must be set up on the router for SDM to use to local login authentication.

After this there are two different ways to install SDM: either locally on the router flash, or through an installer on the user’s computer. Many of the newer routers come with SDM preinstalled, but older routers can be installed with it.

## Security Audit

One of SDM’s main security features is the Security Audit feature. The Security Audit feature can be run in one of two modes: One-Step Lockdown, and Security Audit Wizard. When using the One-Step lockdown, the SDM will automatically lockdown the router based on a list of common security threats. When using the Security Audit Wizard feature, SDM will ask for the changes that you want to be fixed.

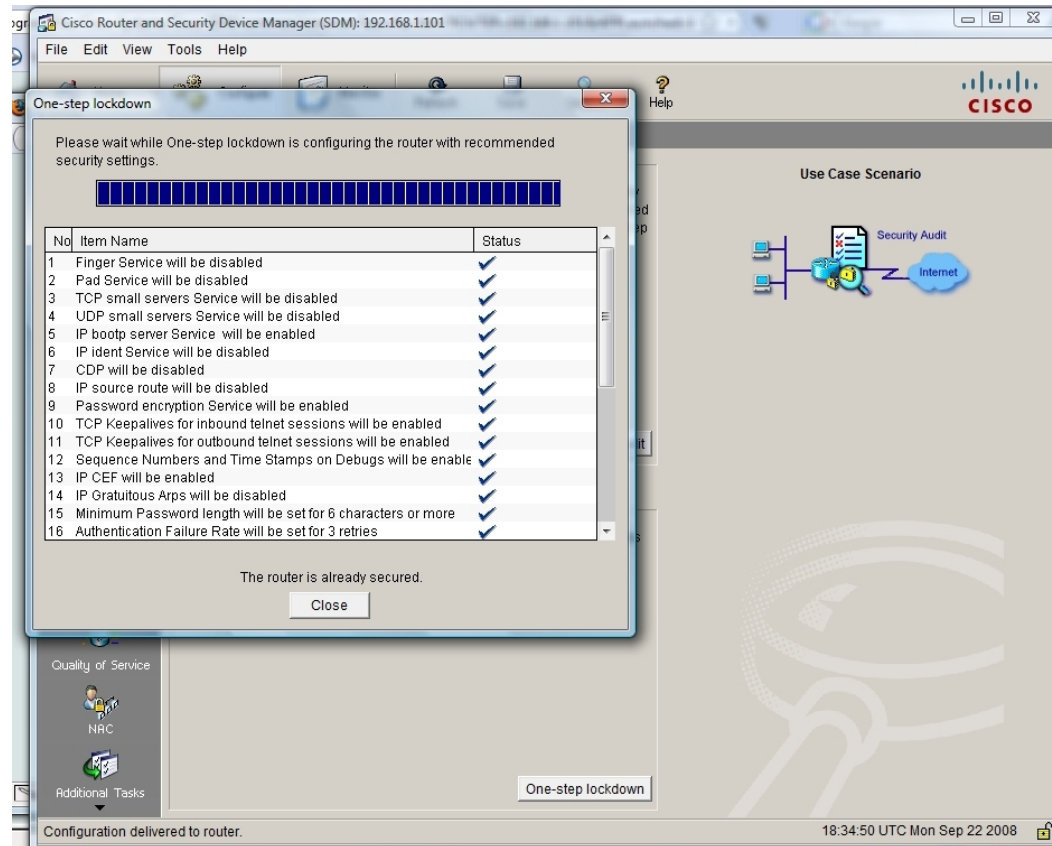


Figure 1 - One-Step Lockdown



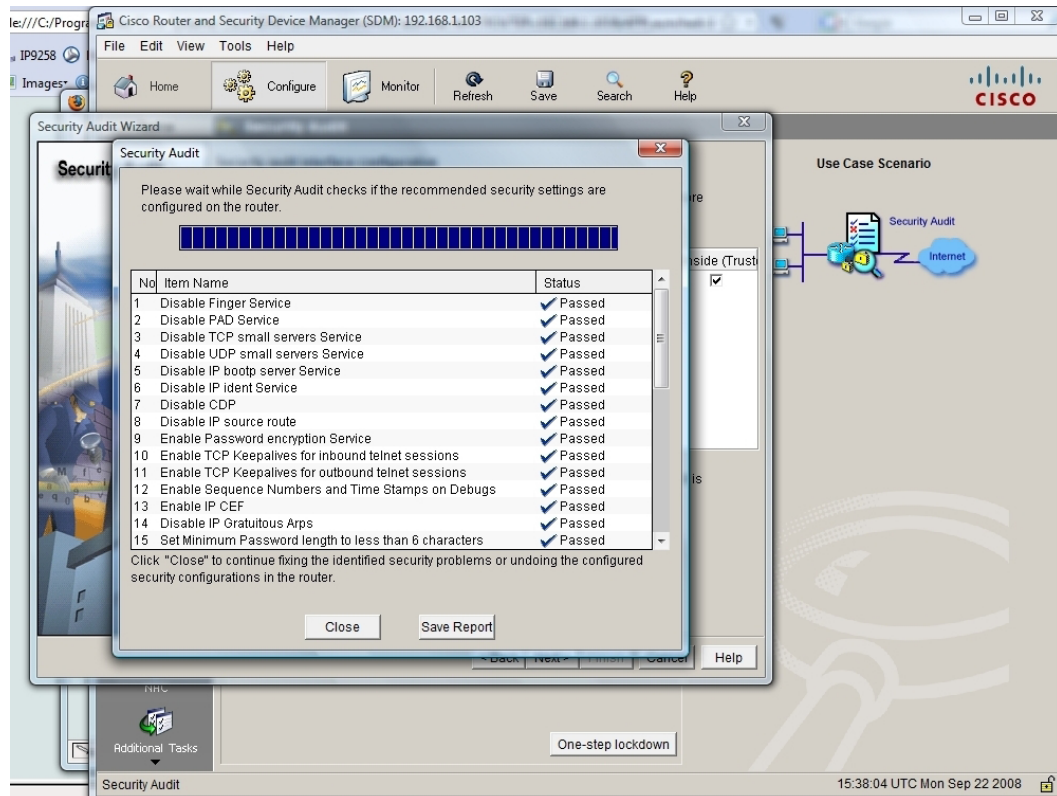


Figure 2 - Security Audit Wizard

## Securing Passwords

One of the easiest ways to ensure security on a Cisco router is by setting passwords. There are a number of different password types which are configurable on a router:

- Enable Password
- Enable Secret Password
- Line Passwords
  - Console Password
  - Auxiliary Password
  - vty Password
- Local User Passwords

### Enable Password

“Enable Password” is used when trying to enter the “Enable Configuration” mode.

```
router(config)#enable password password
```

## Enable Secret Password

“Enable Secret Password” is used when trying to enter the “Enable Configuration” mode. The difference between “Enable Password” and “Enable Secret Password” is the password’s security in the router’s configuration. When using “Enable Password,” it is stored in the configuration files in one of two ways: clear text, or using Cisco-Proprietary encryption. The problem with the Cisco-Proprietary encryption is that it is easily reversible and therefore not secure. When using the “Enable Secret Password” method, the password is entered in the configuration as an MD5 hash and therefore is not reversible and is highly secure.

```
router(config)#enable secret password
```

## Line Passwords

Line passwords are used to secure specific entry points into the router. The three main types include console, auxiliary, and vty passwords. The console password is used to secure the console access into the router. The auxiliary password is used to secure the access through the router auxiliary port. The vty password is used to secure the telnet and/or ssh virtual entry points coming into the router.

```
router(config-line)#login  
router(config-line)#password password
```

## Local User Passwords

“Local User Password” is used when individual users are set up on the router. Like “Enable Password,” user passwords can be entered using either a clear text password, Cisco-Proprietary encrypted password, or using an MD5 hash.

```
router(config)#username username password password  
router(config)#username username secret password
```

## Password Recovery

An important part of being familiar with passwords is knowing how to recover them. This can be done on most Cisco equipment once physical access is possible. If routers are going to be put into a location which is not as physically secure as possible, the option to disable this ability is possible through configuration. It should be noted however that if password recovery is disabled in the configuration and the password is lost, the configuration will not be recoverable from the router and must be stored elsewhere.

```
router(config)#no service password-recovery
```

## Configuring Cisco Password Encryption

As described above, a method of masking the passwords in the configuration is to use the Cisco-Proprietary encryption algorithm. By default, this is enabled and masks the password, however it is easily reversible.

```
router(config)#no service password-encryption
```

## Configuring Miscellaneous Password Parameters

There are a number of different parameters which can be configured to affect different password behaviors. The first one shown below is where you can configure the minimum length of the passwords used on the router.

```
router(config)#security password min-length length
```

The second one shown is how you can configure the number of login attempts before a 15 second delay is imposed. By default, this parameter is set to 10 login attempts.

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

The third one shows how to configure the login inactivity timer. When the time is up, the router will automatically log the person out. By default, this timer is set for 10 minutes.

```
router(config)#exec-timeout minutes seconds
```

## Privilege Levels

By default, users logged in using the **enable** command have a privilege level of 15 and can use all commands available on the router. If finer granularity is required, it is possible to setup different privilege levels, so that certain commands can be used and other commands are still restricted. The following shows the two commands that are required to setup the commands into a specific privilege levels.

```
router(config)#privilege exec level level command
```

```
router(config)#enable secret level level password
```

## Role-Based CLI

Another way of configuring multiple levels of access is through Role-Based CLI or Interface views. In order to set this up there are a couple of main commands which are required. The initial two shown are used to setup Authentication, Authorization and Accounting (AAA) and to setup the root view which is used by the senior administrators.

```
router(config)#aaa new-model  
router(config)#enable view
```

The next command is used to setup a custom view which is configured with a separate password.

```
router(config)#parser view view-name  
router(config)#secret password
```

At this point you are ready to configure the commands which are to be allowed in a specific view.

```
router(config)# commands parser-mode {include | include-exclusive | exclude} [all] command
```

## Securing IOS Images and Configuration Files

Cisco calls the router image and configuration the *bootset* and the Cisco IOS Resilient Configuration feature can be used to secure a copy of these files. This feature can only be disabled from the CLI on the Cisco router. The following commands are used to enable these features:

```
router(config)#secure boot-image  
router(config)#secure boot-config
```

The boot image can be restored by booting into ROMmon and using the **boot** command. The secured configuration can be restored using the following command:

```
router(config)#secure boot-config restore restore-filename
```

## Login Banner

Implementing a legally worded login banner is recommended for a secured device. This should be crafted from your legal department and warn of the repercussions of attempting a breach of the networking equipment. It should not, however, have any identifying markings for a specific company or piece of networking equipment. This banner is configured using the following command:

```
router(config)#banner motd delimiter message delimiter
```

## Domain 3 - Implement AAA on Cisco routers using local router database and external ACS

### *Authentication, Authorization and Accounting (AAA)*

AAA is one of the core concepts to know when implementing security on Cisco devices. Each of these items has its own part of the security picture and each should be configured to secure a device. These three are detailed as follows:

- Authentication – The process where users and administrators prove who they are before being able to access a system.
- Authorization – The process where users and administrators are authorized access to specific resources or commands.
- Accounting – The process where the activities which happen on a device are logged in detail and provide a clear record of what each user and administrator did while logged in. Accounting is commonly used for billing or security logging.

### AAA Configuration

There are a number of different commands which are used to configure specific AAA functionality. These will be separated in to three different sections in this manual.

The one command which is universal to all sections of AAA is the command to enable AAA:

```
router(config)#aaa new-model
```

### Authentication

The main procedure for setting up authentication is as follows:

1. Enable AAA.
2. Setup security server configuration. (If used, see later in the domain.)
3. Create an authentication method list.
4. Apply the authentication method list.

There are a number of different commands which can be used to configure authentication depending on how you want the authentication to work. The following is a list of the commonly available authentication commands, which would all be entered in global configuration mode:

- **aaa authentication banner** – Used to create a personalized login banner.
- **aaa authentication enable default** – Used to create an authentication list which is used when trying to access privileged command levels.
- **aaa authentication fail-message** – Used to create a message which will be displayed when a user login fails.
- **aaa authentication local-override** – Used to enable the check of local user database authentication before using other methods of authentication.
- **aaa authentication login** – Used to create an authentication list which is used when logging in to a device.
- **aaa authentication password-prompt** – Used to change the text displayed when being prompted for a password.
- **aaa authentication ppp** – Used to create an authentication list which is using PPP on an interface.
- **aaa authentication username-prompt** – Used to change the text displayed when being prompted for a username.

When configuring PPP authentication the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authentication enable default method1...method4
```

The **default** parameter which is shown in this command is used to set the default “Enable Authentication” behavior. There are a number of different methods which can be configured; up to four can be configured at the same time and are used in order. The methods which can be specified are listed below:

<b>group radius</b>	The RADIUS server configuration is used for authentication.
<b>group tacacs+</b>	The TACACS server configuration is used for authentication.
<b>enable</b>	The “Enable Password” is used for authentication.
<b>line</b>	The “Line Password” is used for authentication.
<b>none</b>	Uses no authentication.

When configuring login authentication the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authentication login {default | list-name} method1...method4
```

The **default** parameter which is shown in this command is used to set the default login authentication behavior. The *list-name* parameter is used to setup a custom login authentication list which is used in conjunction with the line or interface specific command, which is explained later. There are a number of different methods which can be configured; up to four can be configured at the same time and are used in order. The methods which can be specified are listed below:

<b>enable</b>	The "Enable Password" is used for authentication.
<b>group radius</b>	The RADIUS server configuration is used for authentication.
<b>group tacacs+</b>	The TACACS server configuration is used for authentication.
<b>krb5</b>	Uses Kerberos 5 for authentication.
<b>krb5-telnet</b>	Uses Kerberos 5 Telnet authentication protocol when using telnet to access the device.
<b>line</b>	The "Line Password" is used for authentication.
<b>local</b>	The local user database is used for authentication.
<b>local-case</b>	Uses case sensitive local user authentication.
<b>none</b>	Uses no authentication.

When configuring PPP authentication the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authentication ppp {default | list-name} method1...method4
```

The **default** parameter which is shown in this command is used to set the default PPP authentication behavior. The *list-name* parameter is used to setup a custom PPP authentication list which is used in conjunction with the line or interface specific command, which is explained later. There are a number of different methods which can be configured, up to four can be configured at the same time and are used in order. The methods which can be specified are listed below:

<b>group radius</b>	The RADIUS server configuration is used for authentication.
<b>group tacacs+</b>	The TACACS server configuration is used for authentication.
<b>krb5</b>	Uses Kerberos 5 for authentication.
<b>local</b>	The local user database is used for authentication.
<b>local-case</b>	Uses case sensitive local user authentication.
<b>none</b>	Uses no authentication.

In order to apply the configuration as detailed above on specific interfaces or lines, the following commands are used:

```
router(config-if)#ppp authentication protocol1..protocol2 {default | list-name}
```

```
router(config-line)#login authentication {default | list-name}
```

It should be noted however that if a default method list is created, it is automatically enabled on all interfaces and lines which are not specifically configured with a separate method list.

There are several available protocols which can be used with PPP; all four can be used in one command and are attempted in the order entered. The protocols which are available for the **ppp authentication** command are:

<b>chap</b>	Enables use of the Challenge-handshake authentication protocol (CHAP).
<b>pap</b>	Enables use of the Password Authentication Protocol (PAP).
<b>ms-chap</b>	Enables use of the Microsoft - Challenge-handshake authentication protocol (MS-CHAP).
<b>eap</b>	Enables use of the Extensible Authentication Protocol (EAP).

## Authorization

The main procedure for setting up authorization is the same as authentication and is as follows:

1. Enable AAA.
2. Setup security server configuration. (If used, see later in the domain.)
3. Create an authorization method list.
4. Apply the authorization method list.

There are a number of different commands which can be used to configure authentication, depending on how you want the authorization to work. The following is a list of the commonly available authorization commands, all of which would be entered in global configuration mode:

- **aaa authorization network** – Used to create an authorization list which is used when implementing authorization over network-related services.
- **aaa authorization exec** – Used to create an authorization list which is used when determining a user's ability to run the EXEC shell.
- **aaa authorization commands** – Used to create an authorization list which is used when implementing authorization of all commands at a specific user privilege level. The levels range from 0 to 15.
- **aaa authorization reverse-access** – Used to create an authorization list which is used when implementing authorization for reverse access connections (typically reverse Telnet).
- **aaa authorization configuration** – Used to create an authorization list which is used when downloading a configuration from the AAA server.

When configuring network authorization the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authorization network {default | list-name} method1...method4
```



When configuring exec authorization the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authorization exec {default | list-name} method1...method4
```

When configuring reverse-access authorization the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authorization reverse-access {default | list-name} method1...method4
```

When configuring configuration authorization the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authorization configuration {default | list-name} method1...method4
```

When configuring commands authorization the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa authorization commands level {default | list-name} method1...method4
```

The **default** parameter which is shown in this command is used to set the default login authentication behavior. The *list-name* parameter is used to setup a custom network authorization list which is used in conjunction with the line or interface specific command, which is explained later. There are a number of different methods which can be configured; up to four can be configured at the same time and are used in order. The methods which can be specified are listed below:

<b>group radius</b>	The RADIUS server configuration is used for authorization.
<b>group tacacs+</b>	The TACACS server configuration is used for authorization.
<b>local</b>	The local user database is used for authorization.
<b>if-authenticated</b>	Allows the user to run the specific function as long as they are authenticated.
<b>none</b>	Uses no authorization.

In order to apply the configuration as detailed above on specific interfaces or lines, the following command are used:

```
router(config-if)# authorization {arap | commands level | exec | reverse-access} [default | list-name]
```

```
router(config-line)#ppp authorization {default | list-name}
```

## Accounting

The main procedure for setting up accounting is the same as authentication and authorization and is as follows:

1. Enable AAA.
2. Setup security server configuration. (If used, see later in the domain).
3. Create an accounting method list.
4. Apply the accounting method list.

There are a number of different commands which can be used to configure accounting, depending on how you want the accounting to work. The following is a list of the commonly available accounting commands, all of which would be entered in global configuration mode:

- **aaa accounting system** - Used to enable AAA accounting on all system-level events not associated with users.
- **aaa accounting network** – Used to enable AAA accounting on all network-related service requests.
- **aaa accounting exec** – Used to enable AAA accounting on all EXEC shell sessions.
- **aaa accounting connection** – Used to enable AAA accounting on all outbound connections made from the Network Access Server (NAS).
- **aaa accounting commands** – Used to enable AAA accounting on all commands on a specific privilege level.

When configuring system accounting, the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa accounting system {default | list-name} {start-stop | stop-only | none} group group-name
```

When configuring network accounting, the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa accounting network {default | list-name} {start-stop | stop-only | none} group group-name
```

When configuring exec accounting, the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa accounting exec {default | list-name} {start-stop | stop-only | none} group group-name
```

When configuring connection accounting, the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa accounting connection {default | list-name} {start-stop | stop-only | none} group group-name
```

When configuring commands accounting, the command can be configured in a number of different ways; the general command syntax is as follows:

```
router(config)#aaa accounting commands level {default | list-name} {start-stop | stop-only | none} group group-name
```

The *group-name* parameter is able to be one of two options:

<b>group radius</b>	The RADIUS server configuration is used for accounting.
<b>group tacacs+</b>	The TACACS server configuration is used for accounting.

In order to apply the configuration as detailed above on specific interfaces or lines, the following commands are used:

```
router(config-if)#accounting {commands level | connection | exec} {default | list-name}
```

```
router(config-line)#ppp accounting {default | list-name}
```

## AAA Debug

There are also a number of commands which are used to debug the various types of AAA. These different commands are as follows:

```
router#debug aaa authentication
```

```
router#debug aaa authorization
```

```
router#debug aaa accounting
```

## SDM AAA Configuration

In the newer exams, Cisco appears to be placing more emphasis on the use of SDM with specific configuration processes. In order to configure the same parameters as shown under "AAA Debug", above, within SDM, the figures show the various configuration screens that would be used to configure these items using SDM.

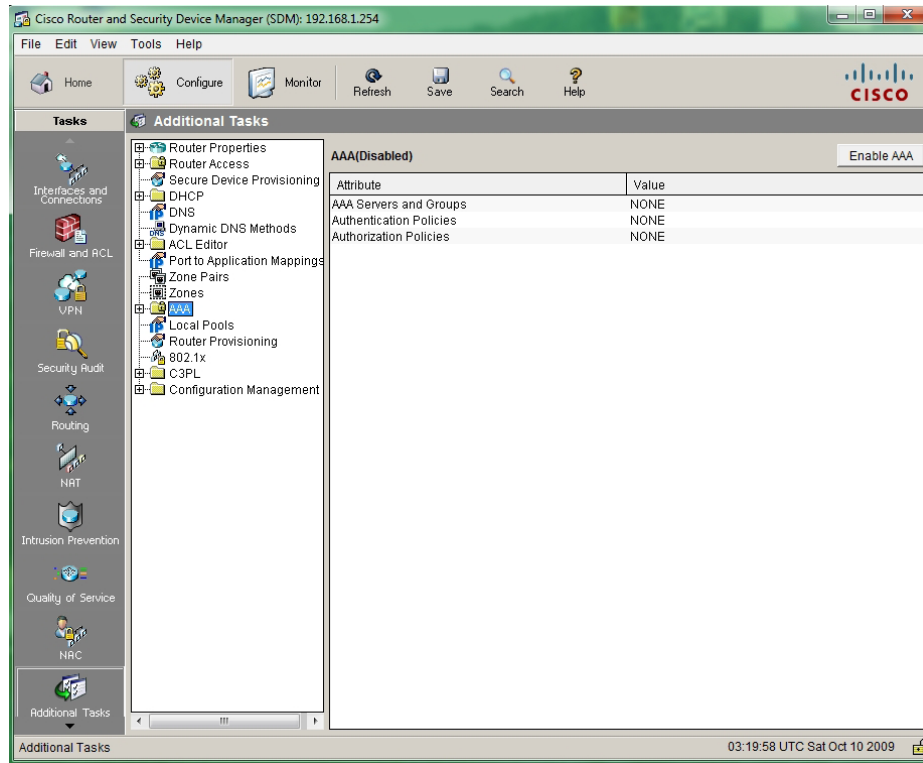


Figure 3 - SDM AAA Screen

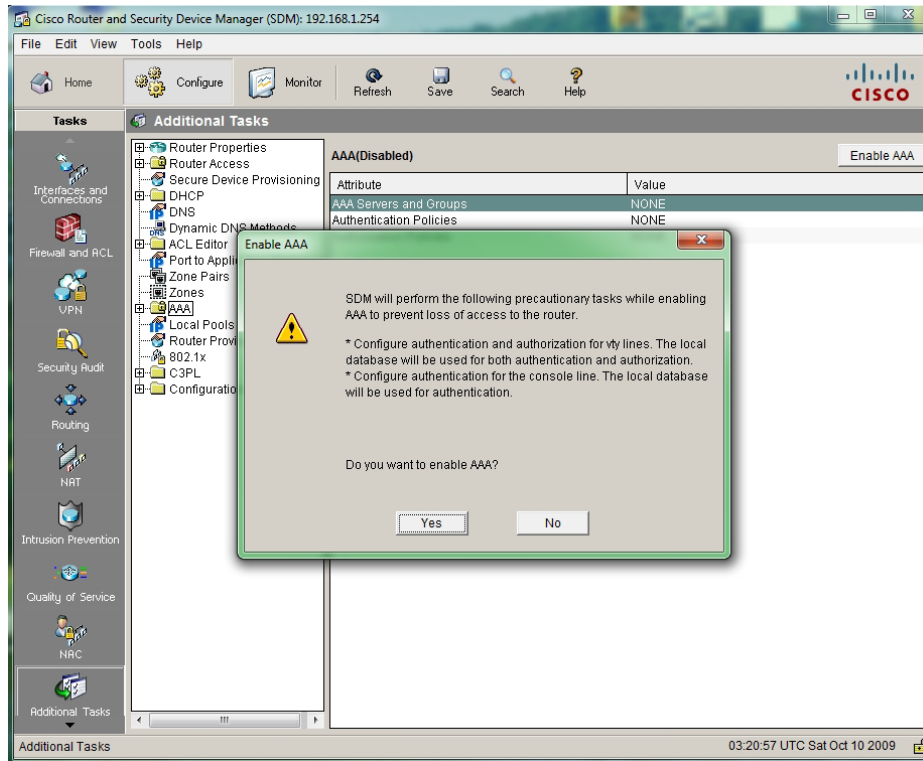


Figure 4 - Enabling AAA with SDM

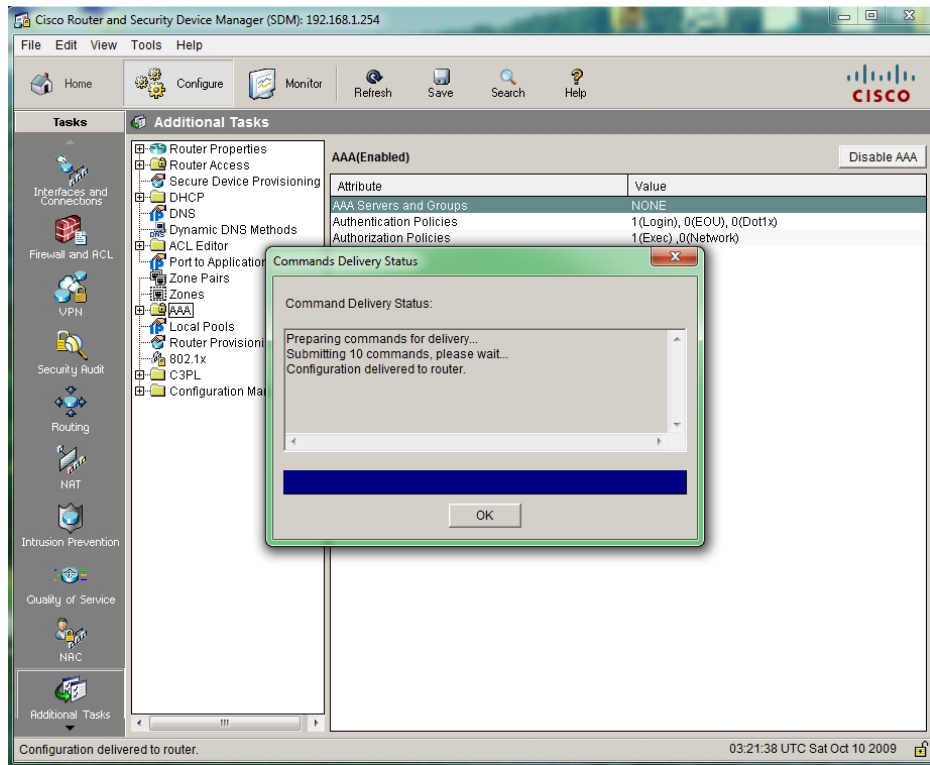


Figure 5 - SDM AAA Enabling Confirmation

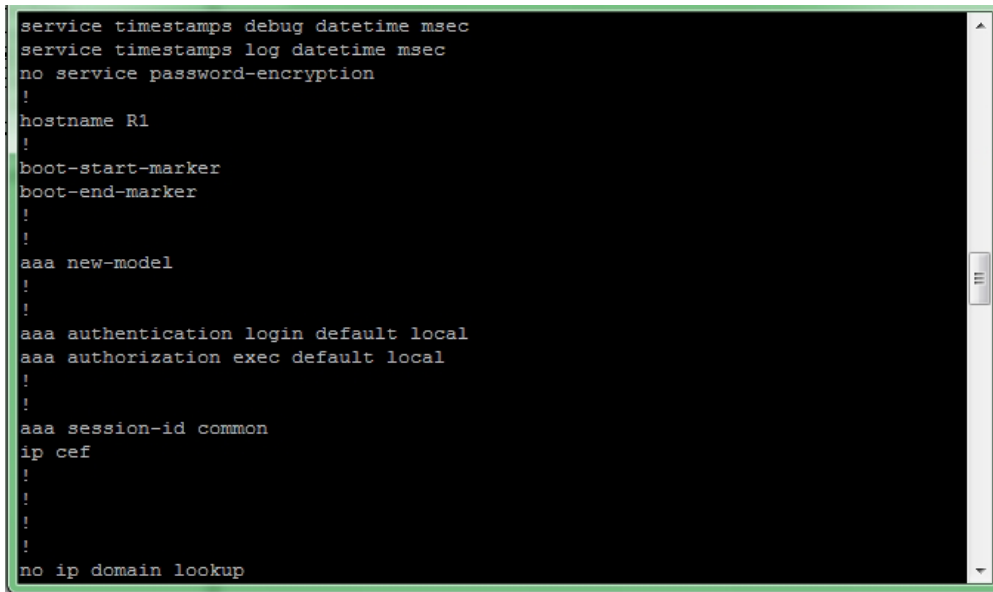


Figure 6 – AAA CLI Configuration from SDM

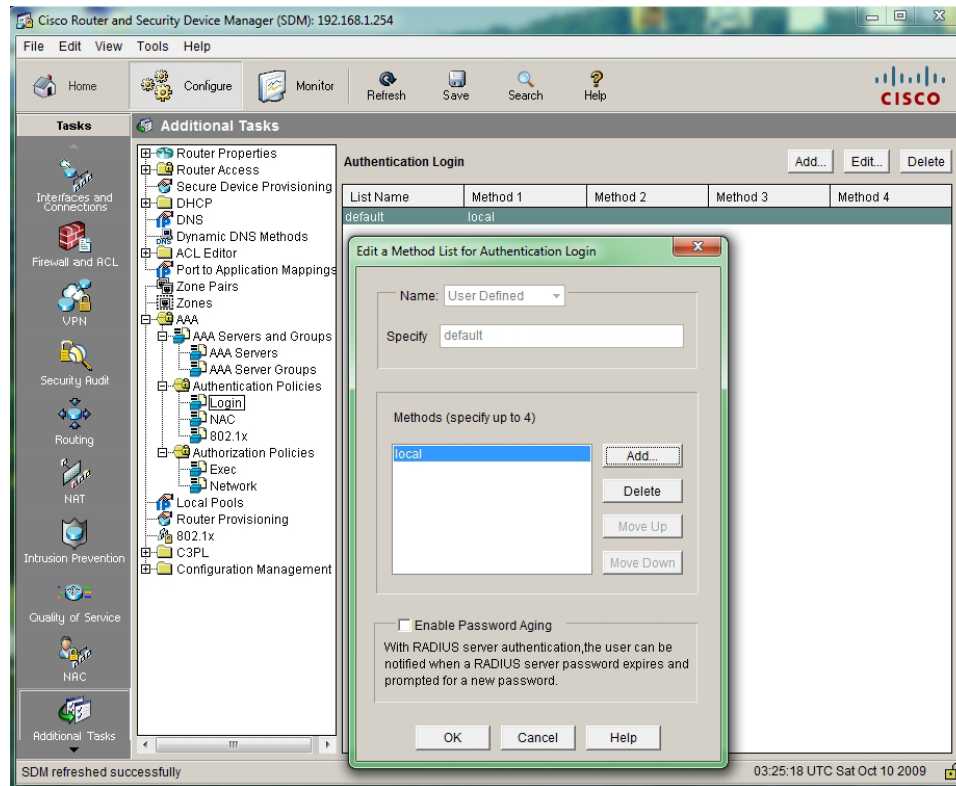


Figure 7 - AAA SDM Method List Editing

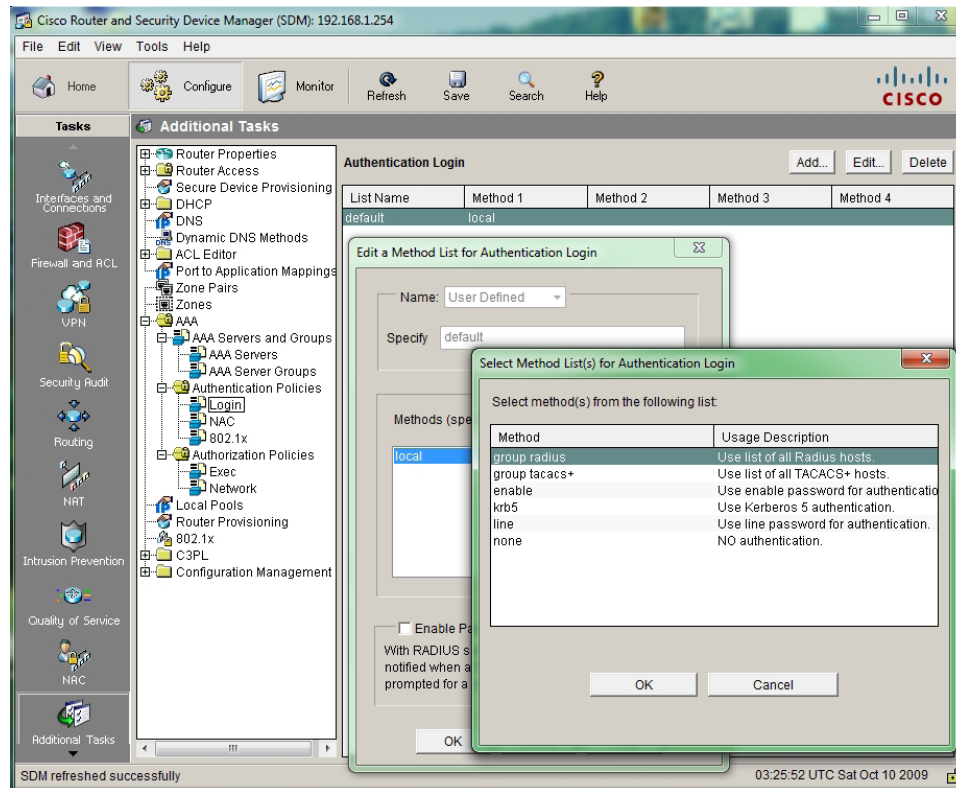


Figure 8 - AAA SDM Method List Adding

## TACACS+ and RADIUS

Two of the most used AAA protocols are Terminal Access Controller Access-Control System (TACACS+) and Remote Authentication Dial In User Service (RADIUS). TACACS+ is a Cisco proprietary which runs on TCP, and RADIUS is an IETF-maintained protocol and runs over UDP. TACACS+ gives some additional functionality which is not supported by RADIUS, including the ability to separate authentication and authorization, and the ability to control the authorization level of users.

### TACACS+ Responses

As the TACACS+ server converses with the user, it uses a couple of responses which determine request outcome:

- **ACCEPT** – The user has been authenticated; authorization begins at this point if configured.
- **REJECT** – Authentication has failed for the user.
- **ERROR** – At some point during the authorization an error has occurred.
- **CONTINUE** – The user is being prompted for further authorization before acceptance or rejection.

### TACACS+ Attributes

There are a number of different attributes which are used for authentication and authorization:

- **ACL** (EXEC authorization) – Lists an access class number that will be applied to a line.
- **ADDR** (SLIP, PPP Authorization) – Used to specify the IP address of the remote host when using a SLIP or PPP connection.
- **CMD** (EXEC) – The attribute-value (AV) pair is used to start an authorization request for an EXEC command.
- **Priv-lvl** (EXEC Authorization) – This is used to specify the current privilege level for command authorization.
- **Route** (SLIP, PPP Authorization) – Used to specify a route to be applied to an interface.
- **InACL** (SLIP, PPP Authorization) – Used to list an inbound ACL for a SLIP or PPP Connection.
- **OutACL** – Used to list an outbound ACL for a SLIP or PPP Connection.
- **Addr-pool** – Used to set the name of the local address pool from which to obtain an address for the remote host.
- **Autocmd** – Used to specify a command which will be automatically executed at EXEC startup.

### RADIUS Message Types

The following are the four message types which are used by a RADIUS server:

- **Access-Request** – Contains AV pairs for username and password which are encrypted by RADIUS.
- **Access-Challenge** – Used for authentication methods which utilize challenge-based approaches.
- **Access-Accept** – Indicates that the user provides information that is correct.
- **Access-Reject** – Indicates that the user provides information that is incorrect.

## RADIUS Attributes

There are a number of different attributes which are used for both authorization and authentication:

- **User-Name**
- **User-Password**
- **CHAP-Password**
- **NAS-IP-Address**
- **NAS-Port**
- **Service-Type**
- **Framed-IP-Address**

## AAA Server Configuration TACACS+ Configuration

There are three main commands which are required for TACACS+ to work. These include:

```
router(config)#aaa new-model
```

This command is used to enable AAA and is shown above as well.

```
router(config-line)#tacacs-server host ip-address single-connection
```

This command is used to setup the connection between the router and the TACACS+ server.

```
router(config-line)#tacacs-server key key
```

This command is used to establish a shared secret encryption key between the TACACS+ server and the router.

## RADIUS Configuration

There are three main commands which are required for RADIUS to work. These include:

```
router(config)#aaa new-model
```

This command is used to enable AAA and is shown above as well.



```
router(config-line)#radius-server host ip-address
```

This command is used to setup the connection between the router and the RADIUS server.

```
router(config-line)#radius-server key key
```

This command is used to establish a shared secret encryption key between the RADIUS server and the router.

## SDM TACACS+/RADIUS Server Configuration

The configuration of both TACACS+ and RADIUS servers are done through the same SDM AAA Server screen.

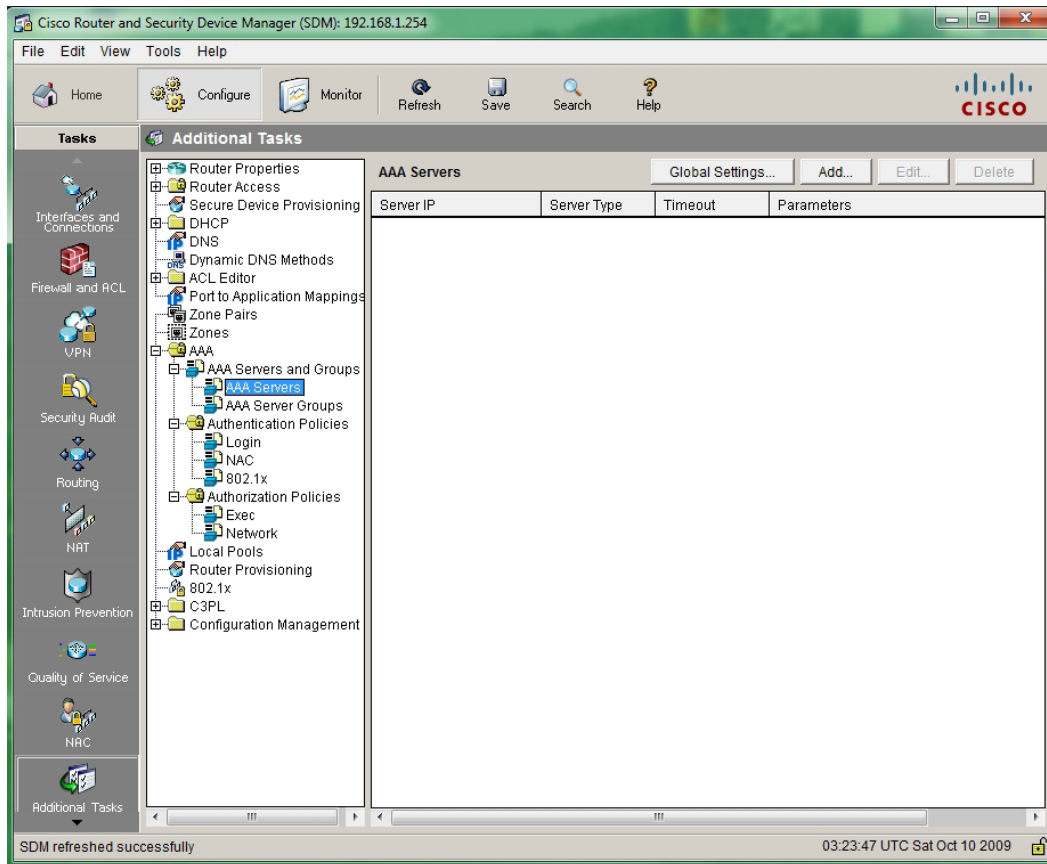


Figure 9 - SDM AAA Server Screen

To add the specific configuration through SDM you use the Add button and provide the appropriate AAA Server details.

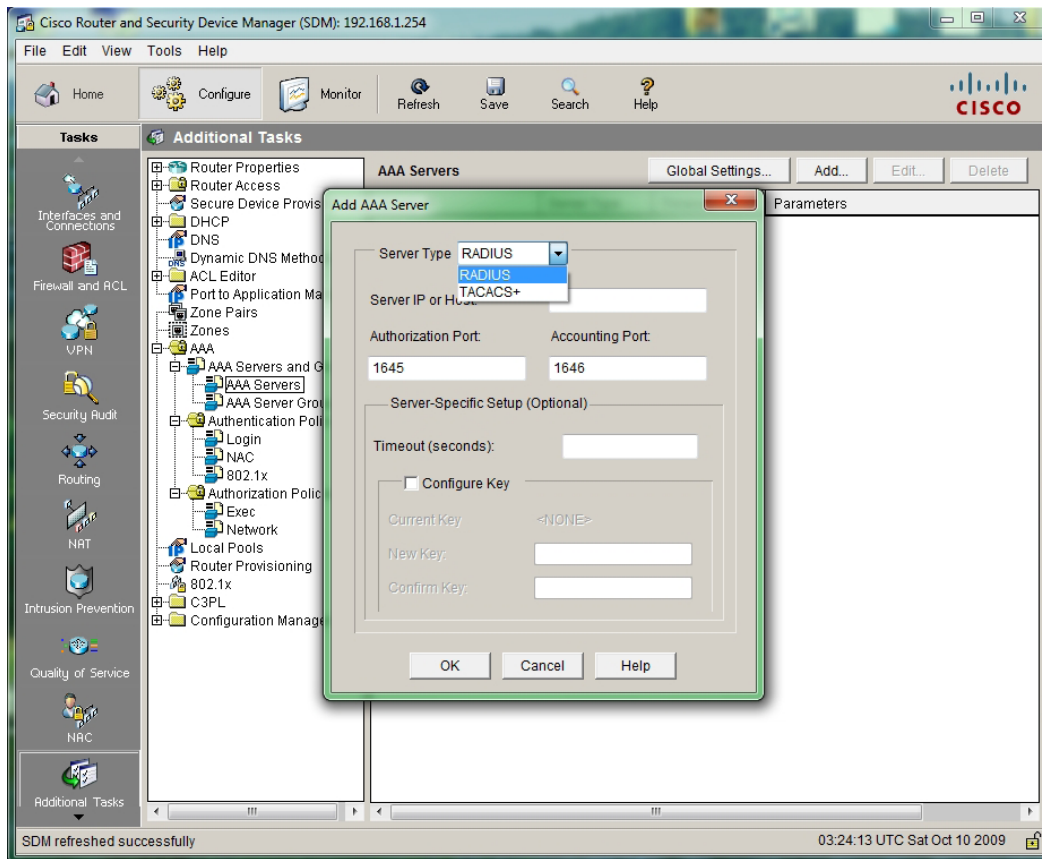


Figure 10 - Adding an AAA SDM Server

## Cisco Secure ACS

Cisco Secure ACS version 4.2 is Cisco's Network Access Server solution. It provides a number of functions including the management and administration of user access to IOS, WPN, firewalls, VoIP and Cisco wireless solutions, to name a few. It also can act as an 802.1x server for access control including support for Cisco's Network Access Control (NAC). It can also provide TACACS+ and RADIUS security server functions.

## Cisco Secure ACS Requirements

Cisco Secure ACS runs on a Microsoft Windows server and requires at least Windows 2000 Server SP4 to be installed and work correctly. The server itself has physical requirements which are as follows:

- 1.8 Ghz Pentium 4 or better
- 1 GB of RAM
- 1 GB of hard drive space. (More of the database server is also being run on the same computer.)
- Monitor supporting 800 x 600 with 256 colors or better
- CD-ROM Drive
- 100 Base-T or faster connection

## Cisco Secure ACS Connections

In order for Cisco Secure ACS to communicate with clients it uses specific IP network ports. These are detailed as follows:

Feature	Protocol	Port(s)
RADIUS Authentication and/or Authorization	UDP	1645, 1812
RADIUS Accounting	UDP	1646, 1813
TACACS+	TCP	49
Cisco Secure ACS database replication	TCP	2000
RDBMS Synchronization	TCP	2000
User-Changeable password web application	TCP	2000
Logging	TCP	2001
Administrative HTTP port	TCP	2002
Administrative HTTP port range	TCP	Configurable

## Domain 4 - Mitigate threats to Cisco routers and networks using ACLs

### Access Lists Types

Access Control Lists (ACLs) are used to control the flow of traffic by filtering specific traffic based on configuration. Cisco IP ACL's are divided into two main groups:

- Standard ACL – Used to only filter source IP traffic. Best-practice is to be applied close to the destination.
- Extended ACL – Used to filter both sources and destinations as well as specific services (TCP and UDP ports). Best-practice is to be applied close to the source.

### Access List Configuration

In order to configure an access-list it must first be defined and then applied. In order to define a standard access-list the following command is used:

```
router(config)#access-list access-list-number {permit | deny} source source-wildcard
```

When using this command the *access-list-number* for a standard access-list must be from 1 through 99 or 1300 through 1999. The *source* parameter specifies a host address or the subnet address of a network. The *source-wildcard* parameter can be used to optionally specify a specific subnet using a wildcard mask.

When defining an extended access-list the following command is used:

```
router(config)#access-list access-list-number {permit | deny} protocol source source-wildcard  
destination destination-wildcard operator port
```

When using this command the *access-list-number* for a standard access-list must be from 100 through 199 or 2000 through 2699. The *protocol* parameter is used to specify the protocol which is to be matched. The *source* parameter specifies a host address or the subnet address of a network. The *source-wildcard* parameter can be used to optionally specify a specific subnet using a wildcard mask. The *destination* parameter specifies a host address or the subnet address of a network. The *destination-wildcard* parameter can be used to optionally specify a specific subnet using a wildcard mask. The *operator* parameter can be optionally used to specify a specific *port*; it can be **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). The *port* parameter specifies a specific port; these can be a specific number or the name of the service.

Another way to configure access lists is using named ACLs. Using this method the access list is configured a little differently. The commands required to setup an access-list this way are as follows:

```
router(config)#ip access-list standard name  
or  
router(config)#ip access-list extended name
```

These first commands create the access-list itself and enter into the access-list configuration mode.

```
router(config)#permit source source-wildcard
```

```
router(config)#deny source source-wildcard
```

These two commands are used when in standard access-list configuration mode and are used similarly to the original access-list commands and parameters.

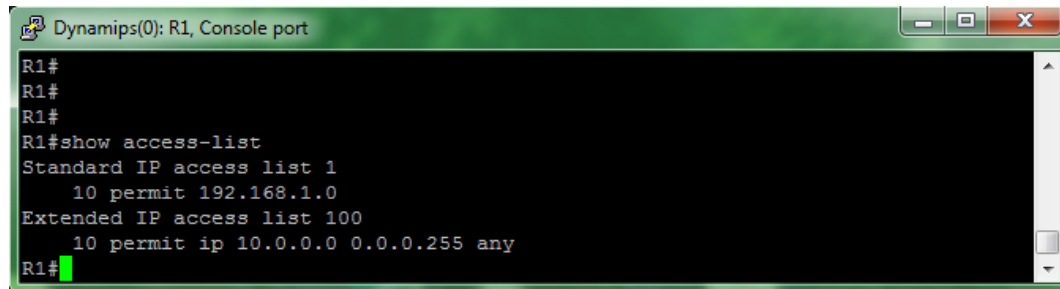
```
router(config)#permit protocol source source-wildcard destination destination-wildcard operator port
```

```
router(config)#deny protocol source source-wildcard destination destination-wildcard operator port
```

These two commands are used when in extended access-list configuration and are used similarly to the original access-list commands and parameters.

In order to display the current access-list configuration, the following command is used:

```
router#show access-list [access-list-number | access-list-name]
```



```
Dynamips(0): R1, Console port
R1#
R1#
R1#
R1#show access-list
Standard IP access list 1
  10 permit 192.168.1.0
Extended IP access list 100
  10 permit ip 10.0.0.0 0.0.0.255 any
R1#
```

Another feature which is available on some routers is the Turbo ACL feature. Using this feature, ACL lookups are optimized in such a way that the fewest number of lookups are performed.

The configuration used to implement the Turbo ACL feature on the supported router is as follows:

```
router(config)#access-list compiled
```

After the ACLs have been defined with the above commands they must then be applied to a specific interface or line. When they are applied to an interface or line they are configured with a specific direction that the access-list will be applied. The two options are as follows:

- Inbound (in) – When applying an access-list inbound, all packets which are received on an interface or line are subject to the access-list configuration.
- Outbound (out) – When applying an access-list outbound, all packets which are transmitted on an interface or line are subject to the access-list configuration.

The configuration that is used to apply the configured access-list is as follows:

```
router(config-if)#ip access-group {access-list-number | access-list-name} {in | out}
or
router(config-subif)#ip access-group {access-list-number | access-list-name} {in | out}
or
router(config-line)#ip access-class {access-list-number | access-list-name} {in | out}
```

### SDM Access-list Configuration

The other method of configuring ACLs is using the SDM interface. The following figures show the different screens which are used to configure ACLs.

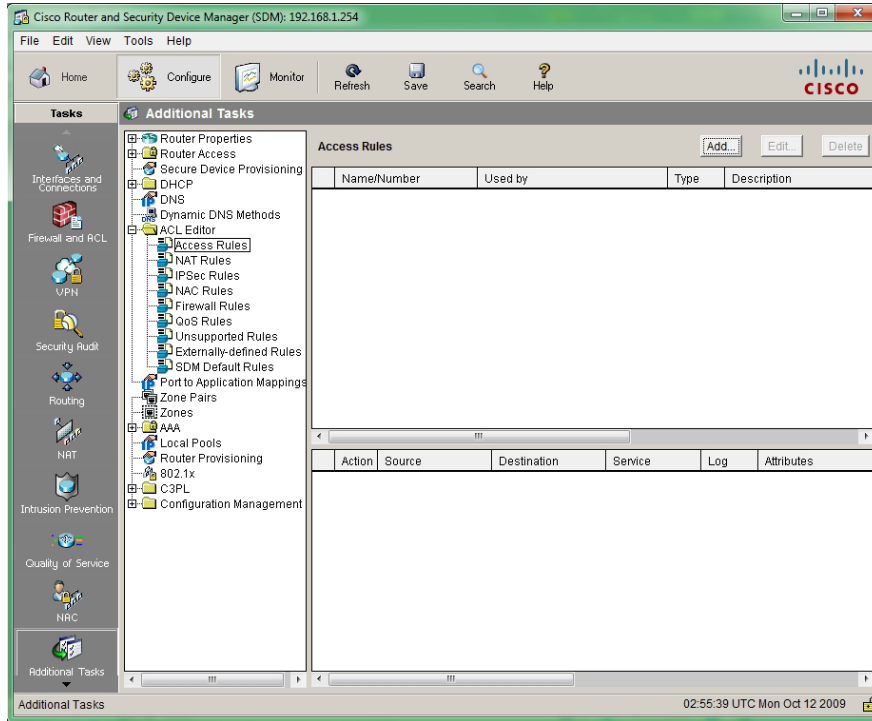


Figure 11 - Initial SDM Access-list Screen

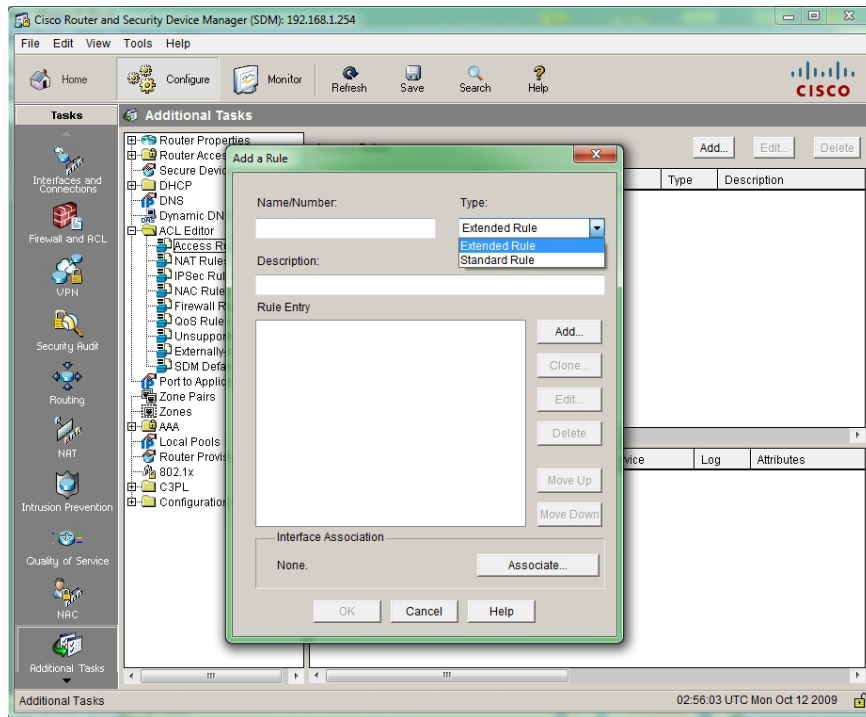


Figure 12 - SDM Access-list Add Screen

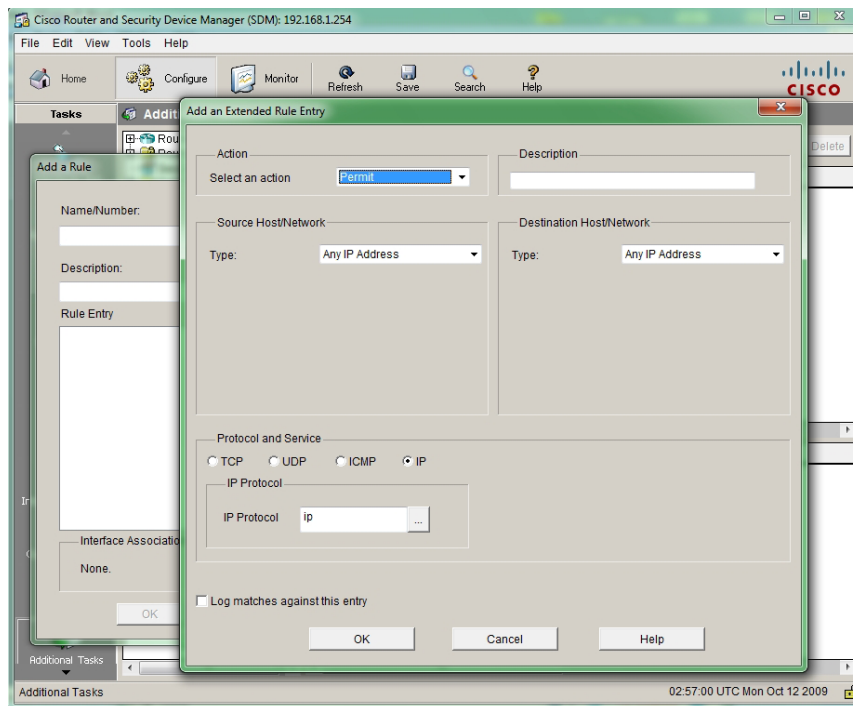


Figure 13 - SDM Access-list Add Rule Screen

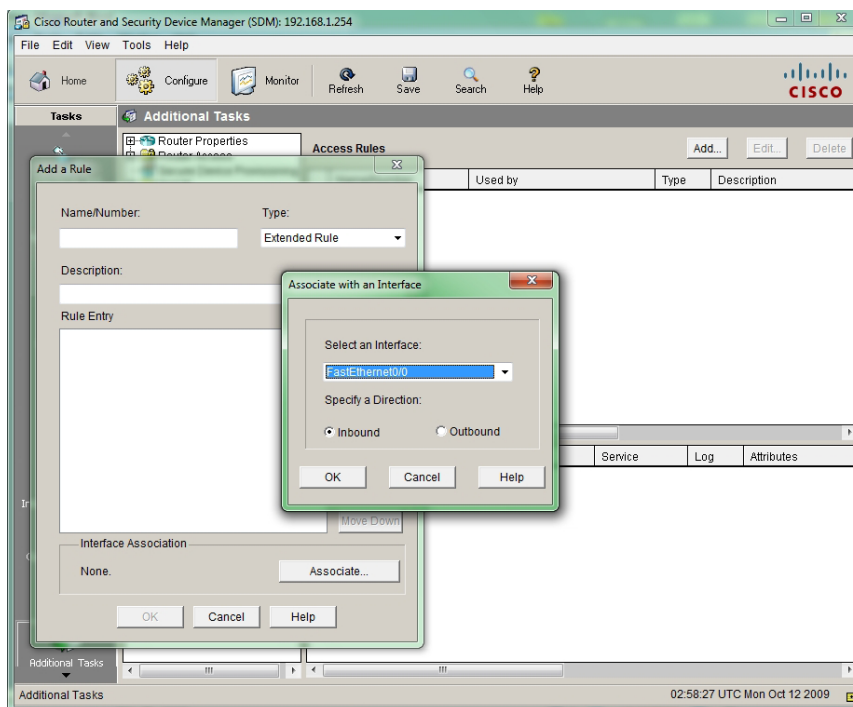


Figure 14 - SDM Access-list Application Screen

## Access List Caveats

As with all features, there are a number of different caveats which must be considered with designing ACLs. The specific access-list caveats are as follows:

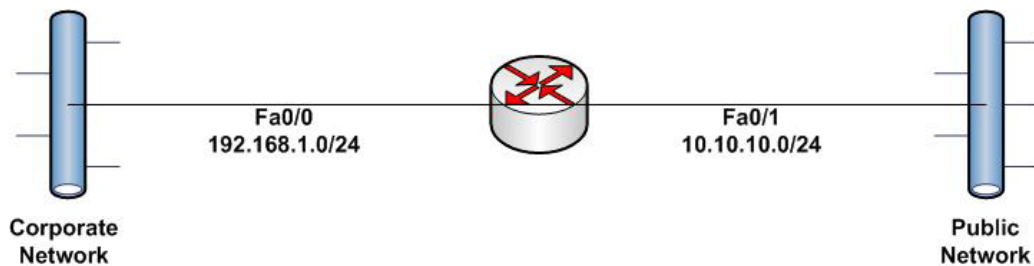
- Implicit Deny.
- Standard ACLs are limited to source address matching.
- ACLs are evaluated in sequential order.
- ACLs are applied directionally.
- Modifying a numbered ACL is hard as new statements are automatically added to the end of the list.

## Preventing IP Spoofing

One of the main things that an ACL can prevent is IP spoofing. In order to perform this you must setup two main ACL statements:

- Ensure internal IP addresses are not being used from the outside interface.
- Ensure external IP addresses are not being used from the inside interface.

The following is a simple sample network diagram:



In this case you want to restrict any traffic from the 192.168.1.0/24 network coming in the Fa0/1 interface and restrict any traffic coming from other than the 192.168.1.0/24 network coming in the Fa0/0 interface. These can be represented as shown below and is applied inbound on the Fa0/1 interface:

```

Dynamips(0): R1, Console port
R1>en
R1#show access-list
Extended IP access list 100
 10 deny ip 192.168.1.0 0.0.0.255 any
 20 permit ip any 192.168.1.0 0.0.0.255
R1#

```



## Domain 5 - Implement secure network management and reporting

### Secure Management and Reporting Planning

There are a number of different things which must be considered when planning for both secure management and reporting on a network. Obviously, the larger the network, the more complex this structure becomes. Also, the larger the network, the more information which can be potentially logged or reported. The following are the Cisco recommendations for designing the best secure management and reporting infrastructure:

- Collection feedback from both network and security team members to determine the best information to be collected.
- Make sure to select an appropriate level of syslog to limit the amount of extra information.
- Secure the transmission and storage of logging information.
- Make use of the Network Time Protocol (NTP) to ensure timestamp synchronization.
- Ensure that all information is logged which may be required by law.
- Allocate sufficient logging storage.
- Identify and implement an enterprise storage system to manage all devices.
- Develop a complete change management solution to track configuration changes.

### Secure Management Architecture

There are two main methods of secure management design:

- In-Band Management – Management traffic is routed through the main production network.
- Out-of-Band Management – Management traffic is routed through an external network designed for management.

### Secure Shell

One of the easiest ways to improve security on a Cisco device is through the replacement of telnet sessions with Secure Shell (SSH). An SSH session is very similar in interaction to a telnet session, with encryption of traffic being the primary difference. There are two versions of SSH which differ in a couple of different ways, including support for different integrity options and key exchange. SSH version 2 requires IOS version 12.3(4)T in order for it to be supported.

## Configuring Secure Shell

The following steps need to be followed in order to correctly configure SSH on a Cisco device.

First, create a username and password combination that you will use to login to the router.

```
router(config)#username username password password
```

Second, enable local login authentication on the vty lines.

```
router(config-line)#login local
```

Third, configure a domain name on the device.

```
router(config)#ip domain-name name
```

Fourth, generate security keys which are used to encrypt traffic.

```
router(config)#crypto key generate rsa
```

When issuing this command a prompt will ask for a key size; it is recommended that this key be at least 1024 bits.

Fifth, specify the use of SSH on the terminal lines.

```
router(config)#transport input ssh
```

There are also a number of parameters which can be set to change the behavior of SSH:

The SSH terminal timeout can be configured from its default of 10 minutes; the *timeout* is entered in seconds:

```
router(config)#ip ssh timeout timeout
```

The number of authentication retries can be changed from its default of 3.

```
router(config)#ip ssh authentication-retries number
```

### Configuring SSH with SDM

The process for configuring SSH with SDM is similar to CLI; the following figures will show the various steps:

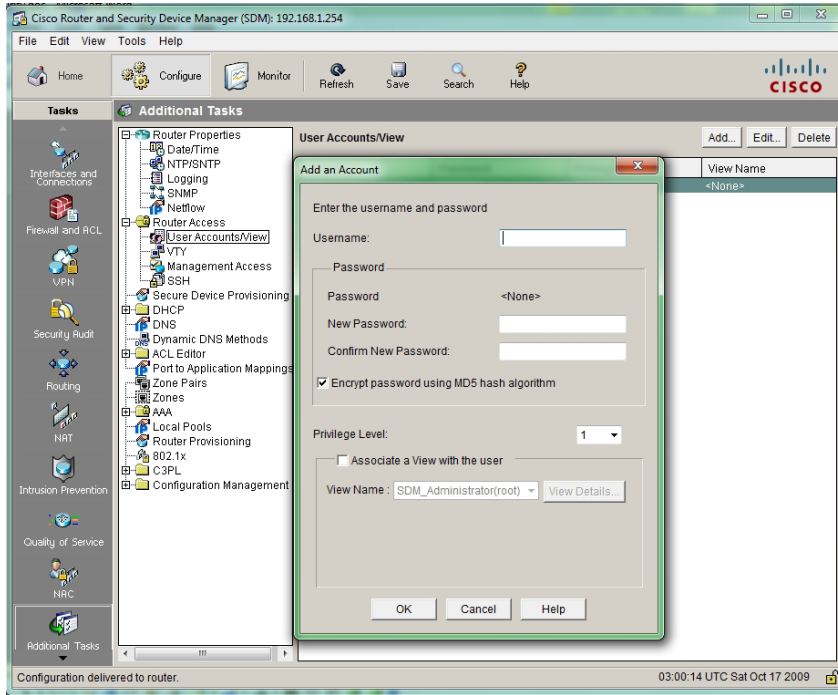


Figure 15 - Create an SSH username/password

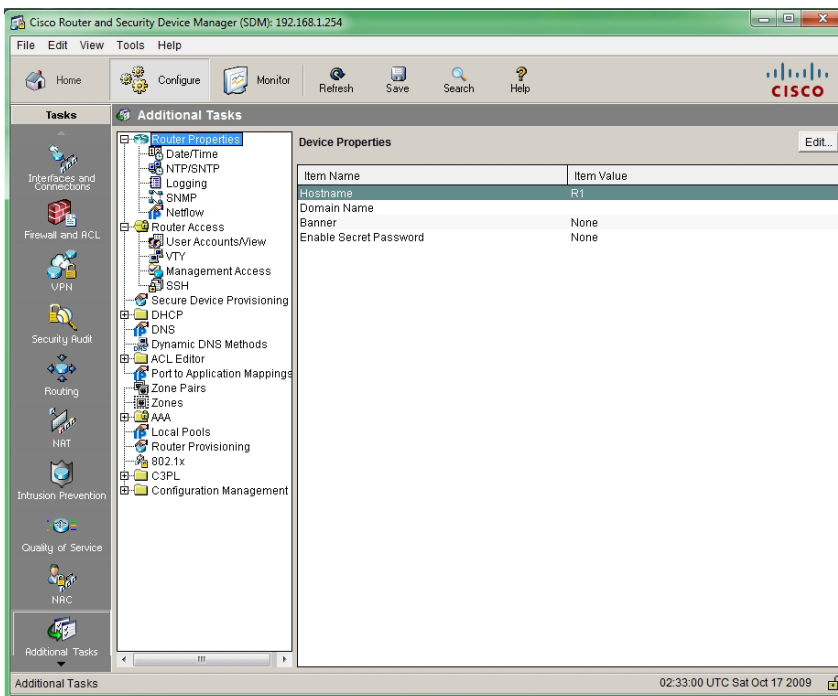


Figure 16 - Goto the Router Properties Screen

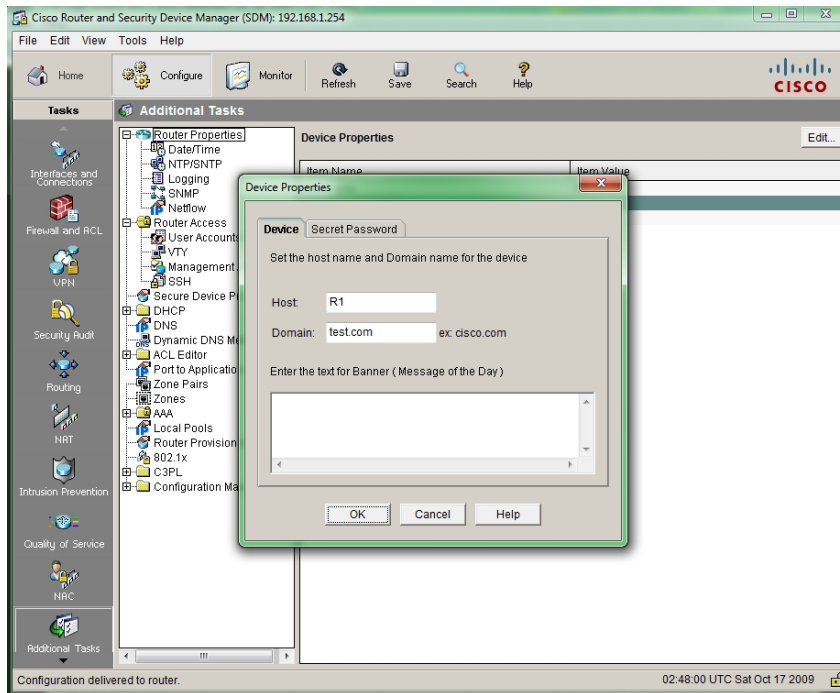


Figure 17 - Set the domain name on the device

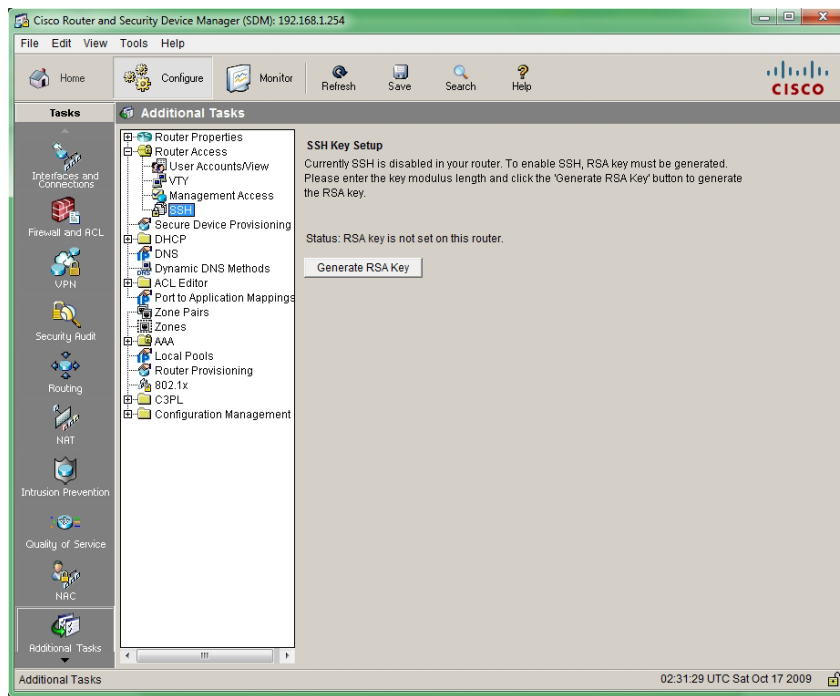


Figure 18 - Goto the SSH screen under Router Access

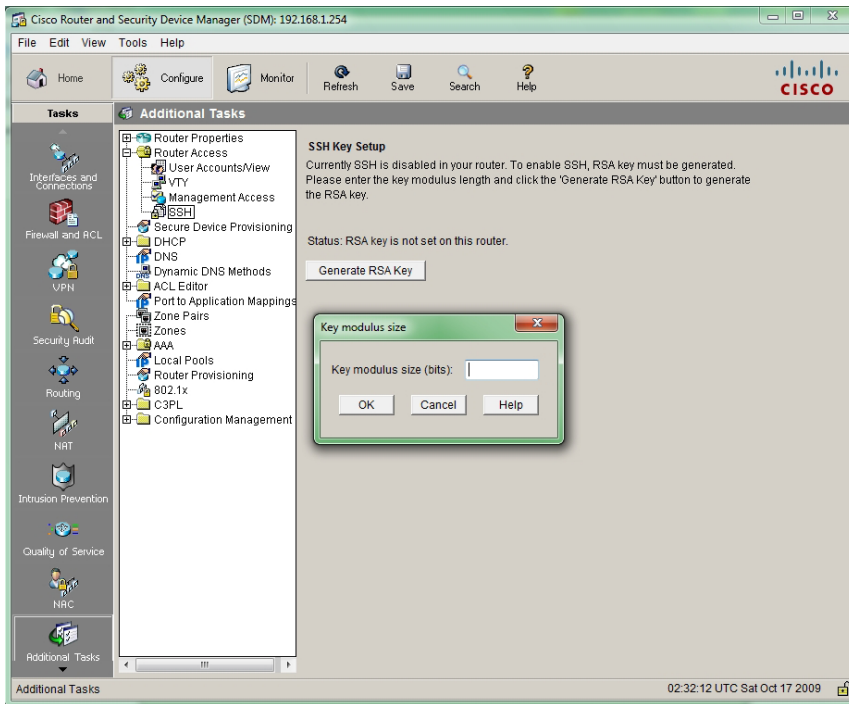


Figure 19 - Set the SSH key size

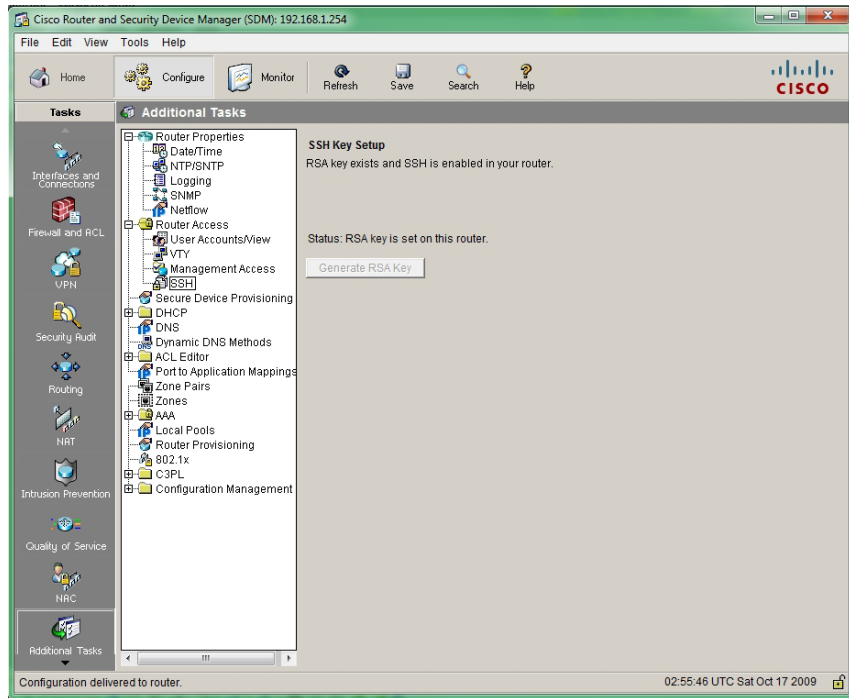


Figure 20 - SSH key generation complete

## Syslog

One of the available options for logging support is through the use of a syslog server for historical logging and alerting purposes. A syslog client is configuring to send out logging information to the server and to format it as a syslog message. Syslog offers a number of different severity levels which are used to separate out routine actions from more serious conditions. The following is a list of the syslog severity levels:

Level	Name
0	Emergency
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

SDM can also be used to display the syslog messages coming from a device as shown in the following screen capture:

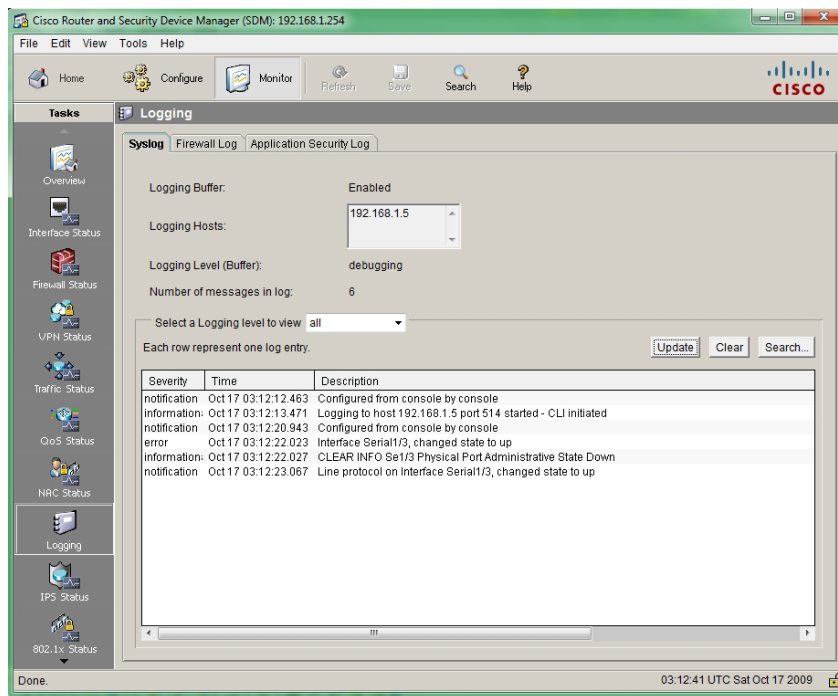


Figure 21 - SDM Syslog messages

## Configuring Syslog

Syslog is easy to configure; it simply requires the following:

First, configure the device to log to a specific syslog server; the *server* parameter can be an IP address or hostname.

```
router(config)#logging host server
```

Second, set the severity of syslog messages to log.

```
router(config)#logging alert severity- level
```

## Configuring Syslog with SDM

The process for configuring syslog with SDM is similar to CLI; the following figures will show the various steps:

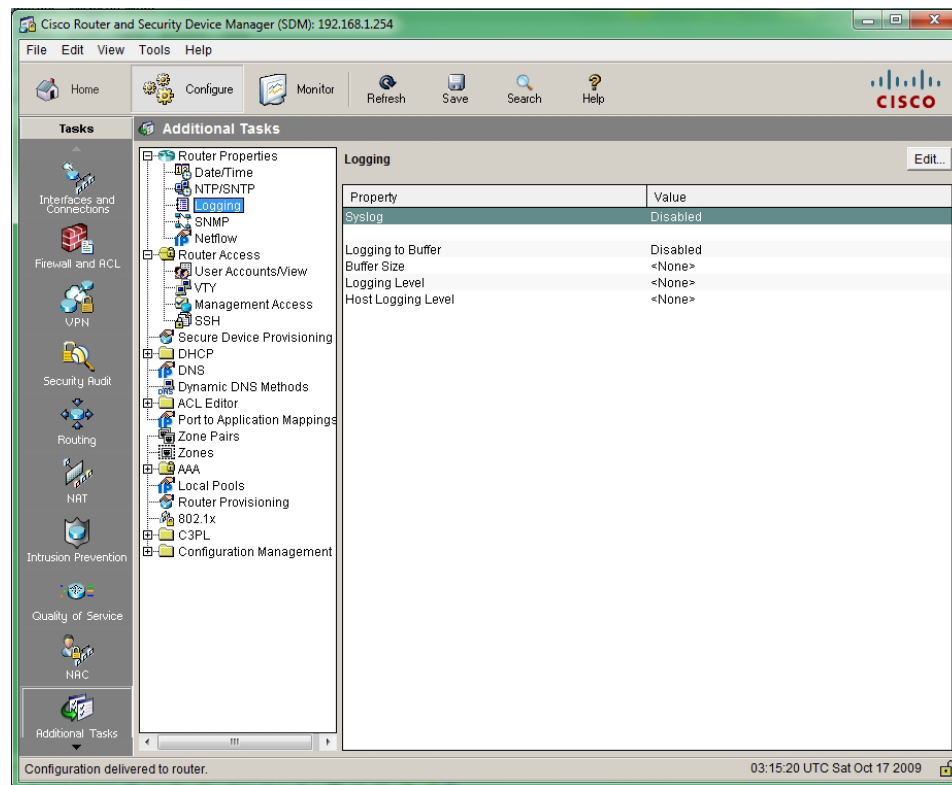


Figure 22 - Enable syslog using the logging screen

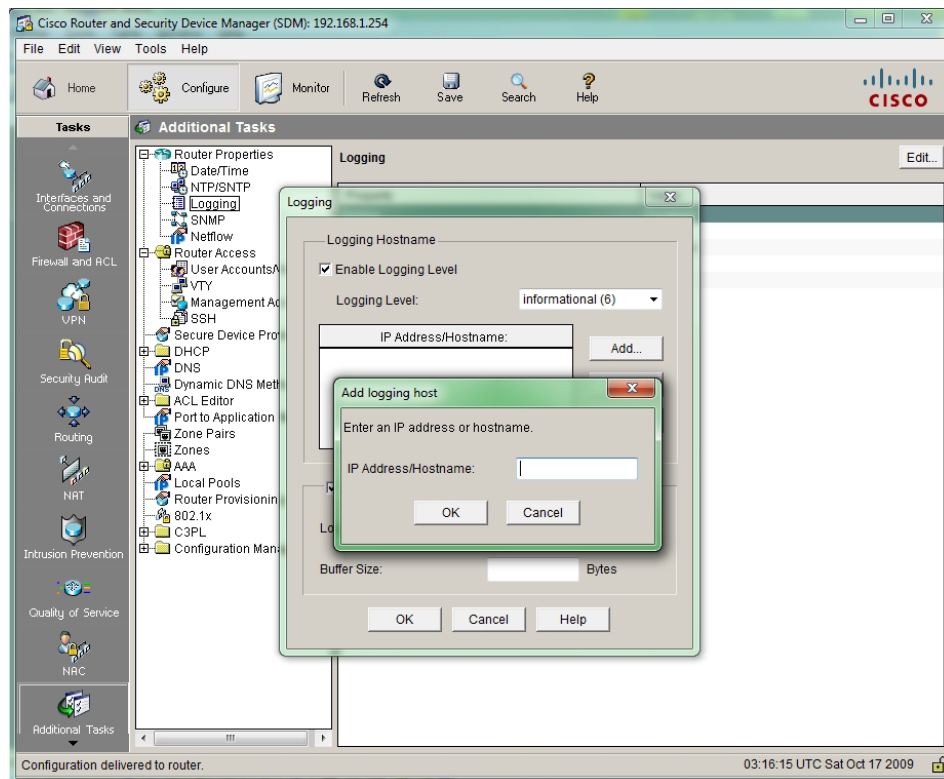


Figure 23 - Add a specific syslog server

## Simple Network Management Protocol (SNMP)

SNMP is the standard network management protocol. Its main purpose is to manage network nodes. There are three versions of SNMP; version 1, version 2c and version 3. Versions 1 and 2c are very similar in security features as neither use encryption or authorization. Version 3 offers both the ability to encrypt the management traffic and authorization.

### SNMP Components

SNMP version 1 and 2c have three main components:

- **SNMP Manager** – This is a role which is taken by the Network Management Server (NMS); it manages the devices and receives any trap information from the devices.
- **SNMP Agent** – The SNMP agent runs on the device and allows the manager to manage the device and sends trap messages to the server, if set up.
- **Management Information Base (MIB)** – A series of objects which hold the information collected for SNMP.



## SNMP Message Types

SNMP sends messages between the manager and the agent; the three main message types are:

- GET – A message used to retrieve information.
- SET – A message used to set a variable on a managed device.
- Trap – An unsolicited message which is sent from the Agent to the Manager which tells of a significant device event.

## SNMP Security Levels

There are three security levels which are defined for SNMP:

- noAuthNoPriv – No authorization or privacy is provided.
- authNoPriv – Authorization is provided but privacy is not.
- authPriv – Both authorization and privacy are provided.

## Configuring SNMP

SNMP version 1 and 2c configuration only requires that the communities be set for SNMP and set trap information.

First, set the SNMP community information.

This command will set the read-only community:

```
router(config)#snmp-server community community RO
```

This command will set the read-write community:

```
router(config)#snmp-server community community RW
```

Second, enable traps on the device.

```
router(config)#snmp-server enable traps
```

Third, set the host to send traps or informs to.

```
router(config)#snmp-server host ip-address/hostname community
```

### Configuring SNMP with SDM

The process for configuring SNMP with SDM is similar to CLI; the following figures will show the various steps:

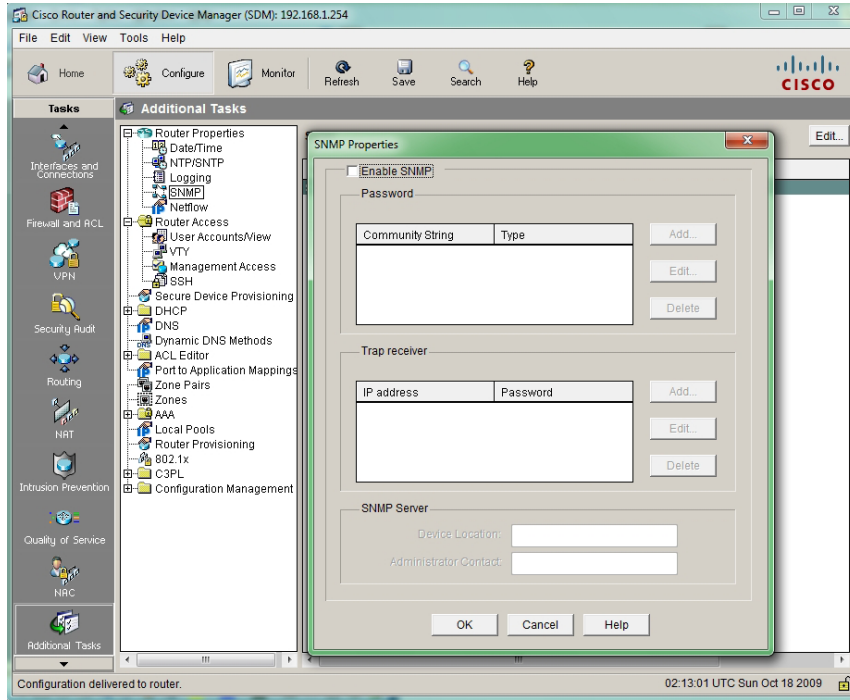


Figure 24 - Enable SNMP

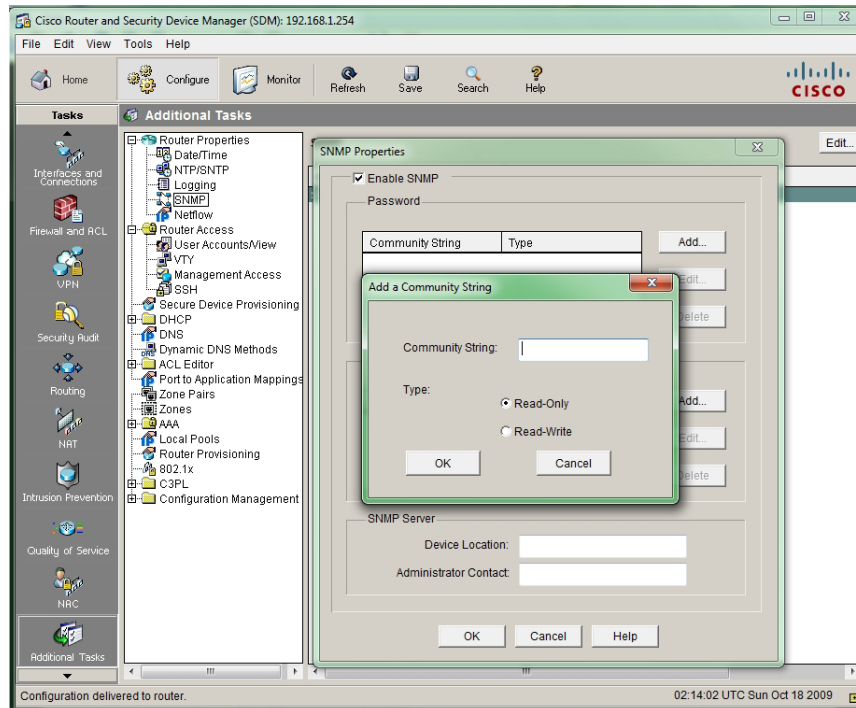


Figure 25 - Setup the community strings

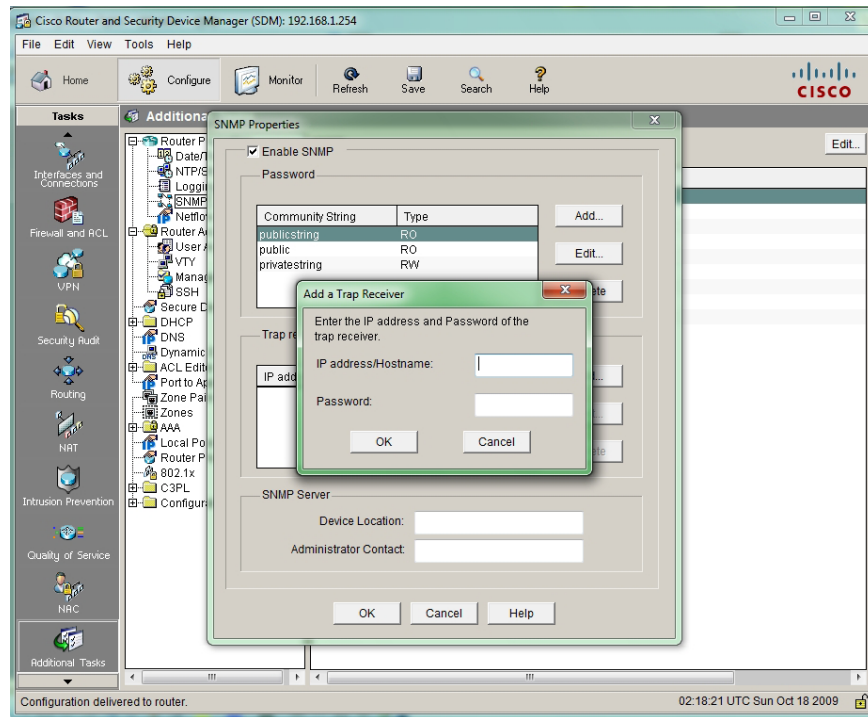


Figure 26 - Setup the trap receiver (Password = community)

## Network Time Protocol (NTP)

NTP is used to synchronize the clocks of the devices on a network so that all network devices have the exact same time. This is very useful for troubleshooting as the logging information from the various devices will be easily correlated to a specific event.

## Configuring NTP

Typical NTP configuration is very easy as it simply requires a command which specifies the server address, and a command to tell the device to synchronize the device.

First, set up the NTP servers which will be used to synchronize time.

```
router(config)#ntp server ip-address/hostname
```

Second, set the device to synchronize with the server.

```
router(config)#ntp update-calendar
```

## Configuring NTP with SDM

The process for configuring NTP with SDM is similar to CLI; the following figures will show the various steps:

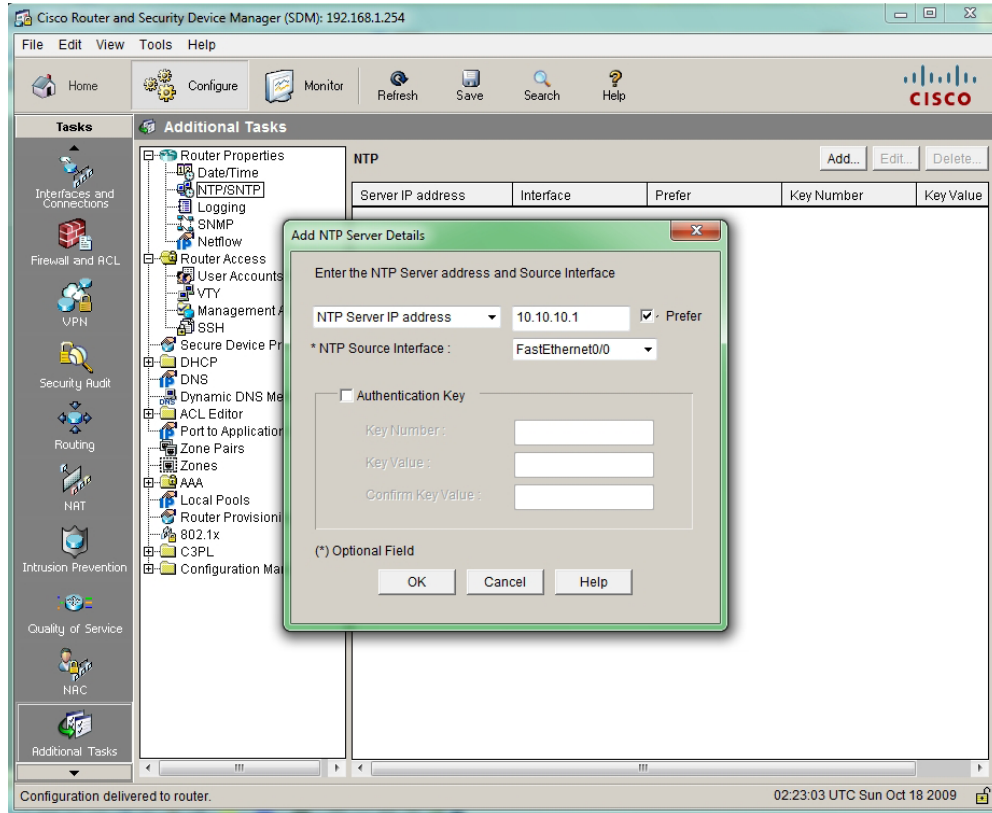


Figure 27 - Add the NTP server

## Domain 6 - Mitigate common Layer 2 attacks

### VLAN Hopping

There are two different types of attack which are both classified as VLAN hopping: Switch spoofing and Double Tagging. Switch spoofing is when someone tries to impersonate a switch on your network in order to collect the layer 2 topology information for your network from your switches. Double Tagging is a method that is used to try and gain access to a restricted VLAN through the double VLAN tagging of a frame.

### Configuring VLAN Hopping prevention

#### Switch Spoofing

Whenever an attacker tries to impersonate a switch they typically gain physical access to a port on one of your switches and try to impersonate a switch on this port. The best way to get around this type of attack is to allow only the specific ports slated for trunking to be able to become trunks. This is done by statically configuring all user or access ports to be only access ports and to configure trunk ports only when they are physical ready to be trunked with another switch.

In order to statically put a port into access mode the following command is used:

```
router(config-if)#switchport mode access
```

In order to statically configure a port to be a trunk the following command is used:

```
router(config-if)#switchport mode trunk
```

It is also good to disable trunking negotiation on trunk ports when statically configuring to port. This is done with the following command:

```
router(config-if)#switchport nonegotiate
```

## Double Tagging

The Double Tagging type of attack requires that the attacker be aware of the native VLAN number which is being used on the network. Without this knowledge the initial switch which receives the altered frame will leave the "outer" or double tag on the frame and the attack would be thwarted. The best way to protect from this attack is through the configuration of a non-standard native VLAN (typically it is set to 1). The following command is used to change this number on an interface:

```
router(config-if)#switchport trunk native vlan vlan
```

## Root Guard

One of the ways that an attacker can try to affect a Spanning Tree network is to hijack the STP root switch. In order to prevent this, Cisco has created the Root Guard feature which transitions a port into *root-inconsistent* state should a superior BPDU be received on a port not coming from in on the root port.

## Configuring Root Guard

In order to configure the Root Guard feature, the following command must be entered on all non-root ports:

```
router(config-if)#spanning-tree guard root
```

## Portfast

One of the methods which can be used to increase the convergence time of spanning-tree is to use the Portfast feature. The Portfast feature works by transitioning directly to forwarding state. That way, the port does not have to progress through the various STP modes to reach the forwarding state, which can take between 30 and 50 seconds.

## Configuring Portfast

The Portfast feature is configured on all access ports which attach to a single user device. This is done with the following command:

```
router(config-if)#switchport portfast
```

## BPDU Guard

BPDU Guard is a feature that works in conjunction with the Portfast feature. Since ports which are configured with Portfast are only suppose to be connected to user devices and not other switches, the BPDU Guard feature works by disabling a port should a BPDU be advertised through a Portfast port.

## Configuring BPDU Guard

Bridge Protocol Data Units (BPDU) are communication messages sent between connected switches for the purpose of configuring and monitoring the Spanning Tree. The BPDU Guard feature is configured on a port which is already configured with Portfast. Because the ports are already assumed to not have a switch attached to them, no BPDUs should ever be seen. BPDU Guard watches for BPDUs on the access ports which indicate a user illegally attached a switch to an access port. The command which is used to configure BPDU Guard is as follows:

```
router(config-if)#switchport portfast bpduguard
```

## DHCP Snooping

One of the features which can be used on a Cisco device is the DHCP Snooping feature, which is used to protect from DHCP server spoofing. This feature works by trusting ports which connect to valid DHCP servers or from a port which is in the direction of a valid DHCP server.

## Configuring DHCP Snooping

The DHCP Snooping feature is configured by first enabling the DHCP Snooping feature and then configuring individual trusted ports.

```
router(config)#ip dhcp snooping
```

```
router(config-if)#ip dhcp snooping trust
```

## Dynamic ARP Inspection (DAI)

Another type of layer two attack which can happen is one aimed at ARP requests. ARP requests are used to locate the IP address of a remote device based on its MAC address. If an attacker was able to spoof a client into believing that they were a valid trusted device, the client could potentially give away trusted information without knowing it. One of the ways to prevent this is through the use of Dynamic ARP Inspection. DAI uses the DHCP snooping binding table to be aware of which clients are able to talk and from which MAC address and IP address they are talking from. Ports are configured to be trusted or untrusted; all ARP replies that come in an untrusted port are compared against the DHCP snooping binding table. If there is a match then the traffic is allowed; if not, then the port is disabled.

## Configuring DAI

Dynamic ARP Inspection (DAI) is configured by enabling it on specific VLANs and then specifying trusted ports. By default all ports are not trusted. Only ports which are known to be trusted and secured should be configured as such.

```
router(config)#ip arp inspection vlan vlan
```

```
router(config-if)#ip arp inspection trust
```

## Port Security

Port security offers the ability to secure a port through a number of different configuration types. This includes limiting the number of MAC addresses allowed on a specific port, the specific MAC address allowed on a port, and the behavior when a port detects a violation.

## Port Violation Behaviors

When port detects a violation it can behave in one of three ways:

- **Protect** – When configured, the port will forward frames from the known MAC addresses allowed on a port to all MAC addresses trying to transit on that port. Any traffic over the allowed amount will be dropped. No notification message is sent if a violation occurs.
- **Restrict** – Exactly the same as Protect except an SNMP trap and syslog message are sent upon violation.
- **Shutdown** – When configured, the port will shutdown on any violation and send an SNMP trap and syslog message.

## Secure MAC Address Types

There are three different types of Secure MAC address on a Cisco device:

- Static Secure MAC Addresses – This type of MAC address is statically configured.
- Sticky Secure MAC Addresses – This type of MAC addresses is dynamically learned and is entered both in the CAM table of the switch and in the running configuration. If the running configuration is saved to the startup configuration, they effectively become statically configured addresses on reload.
- Dynamic Secure MAC Addresses – This type of MAC address is dynamically learned and is entered into the CAM table of the switch but is not saved to the running configuration. This type of address is lost on reload.

## Configuring Port Security

In order to get started with configuring port security it must be first enabled; this is done with the following command:

```
router(config-if)#switchport port-security
```

In order to configure the maximum number of MAC addresses which are allowed on a port, you use the following command:

```
router(config-if)#switchport port-security maximum number
```

In order to change the default port behavior when a violation is detected, the following command is used:

```
router(config-if)#switchport port-security violation behavior
```

By default, the port behavior is to shut down the port.

When you want to set up a static secure MAC address, the following command is used:

```
router(config-if)#switchport port-security mac-address mac-address
```

In order to enable a port to make use of sticky MAC addresses, you use the following command:

```
router(config-if)#switchport port-security mac-address sticky
```



## Domain 7 - Implement the Cisco IOS firewall feature set using SDM

As of IOS version 12.4(6)T Zone-based firewalls have been supported. This type of firewall works by assigning interfaces to a specific zone. All interfaces which are assigned to the same zone are allowed to talk to each other, but interfaces not in the same zone are by default dropped. If traffic is to be allowed between zones this is done unidirectionally from one zone to the other. Configuration through SDM is typically done through a wizard or through statically configuring the zones and zone pairs.

The following figures show how the basic and advanced firewall wizards work to perform this function:

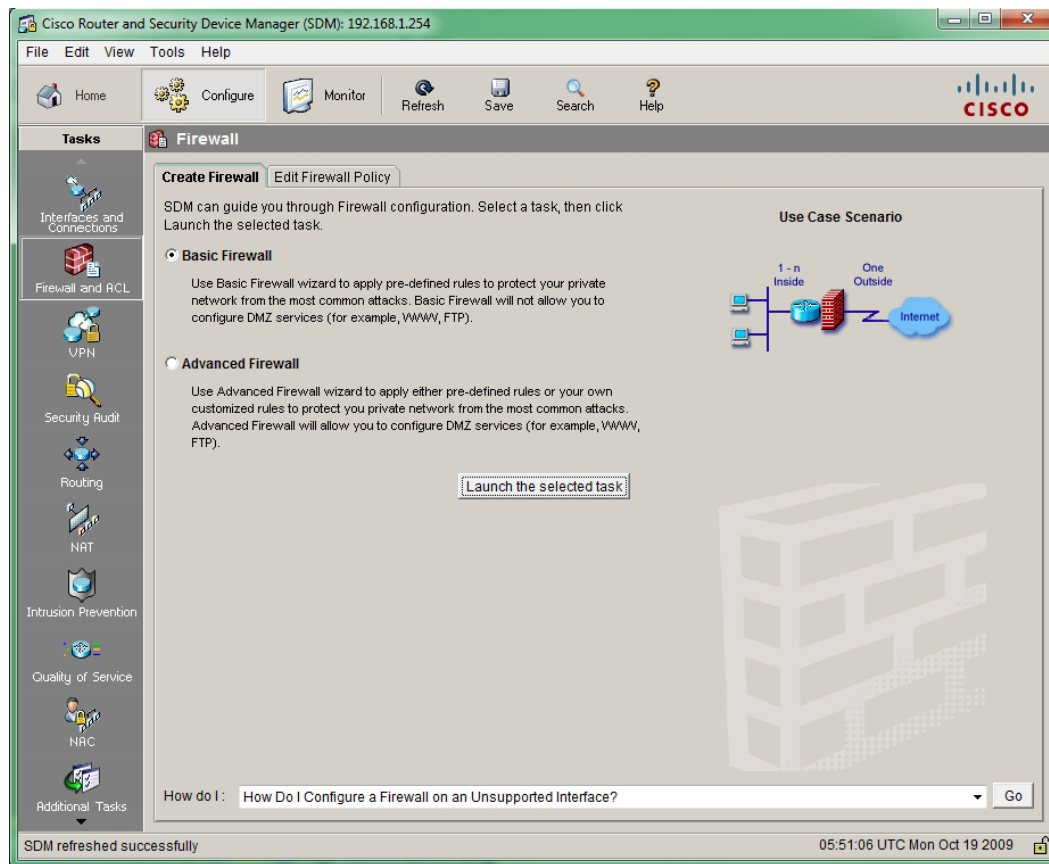


Figure 28 - Main Firewall Screen

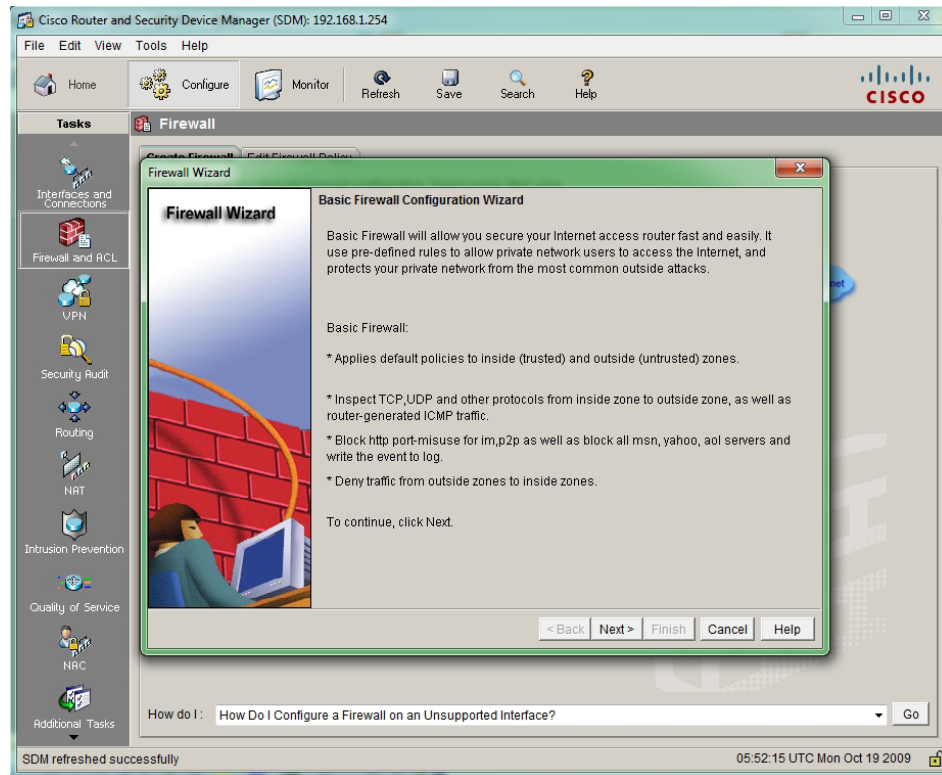


Figure 29 - Basic Firewall Wizard Screen

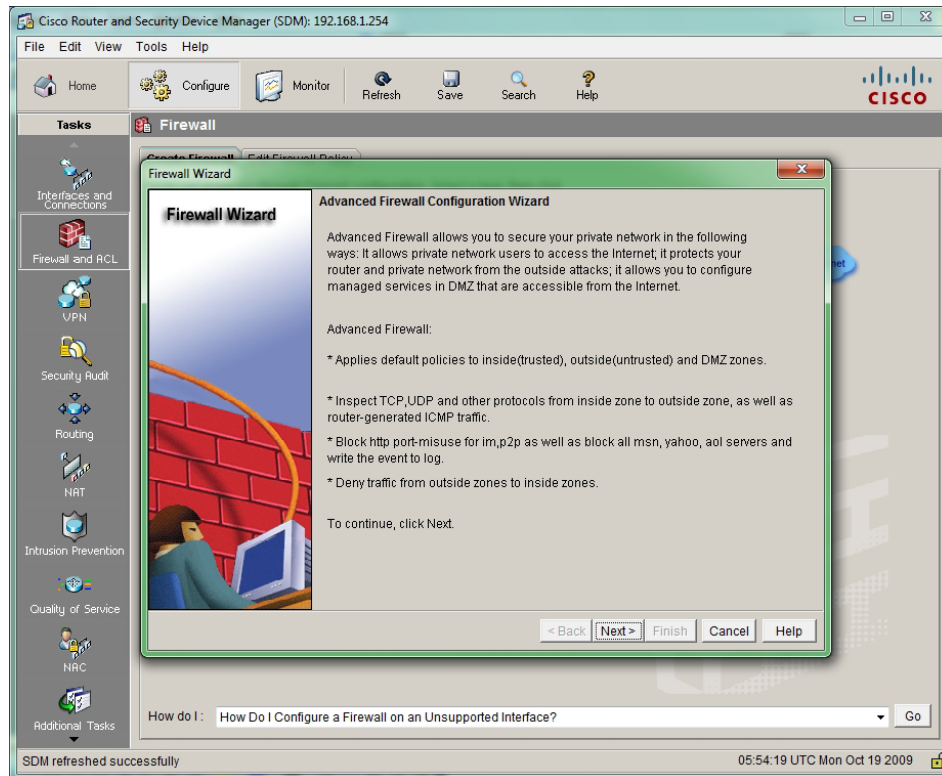


Figure 30 - Advanced Firewall Wizard Screen

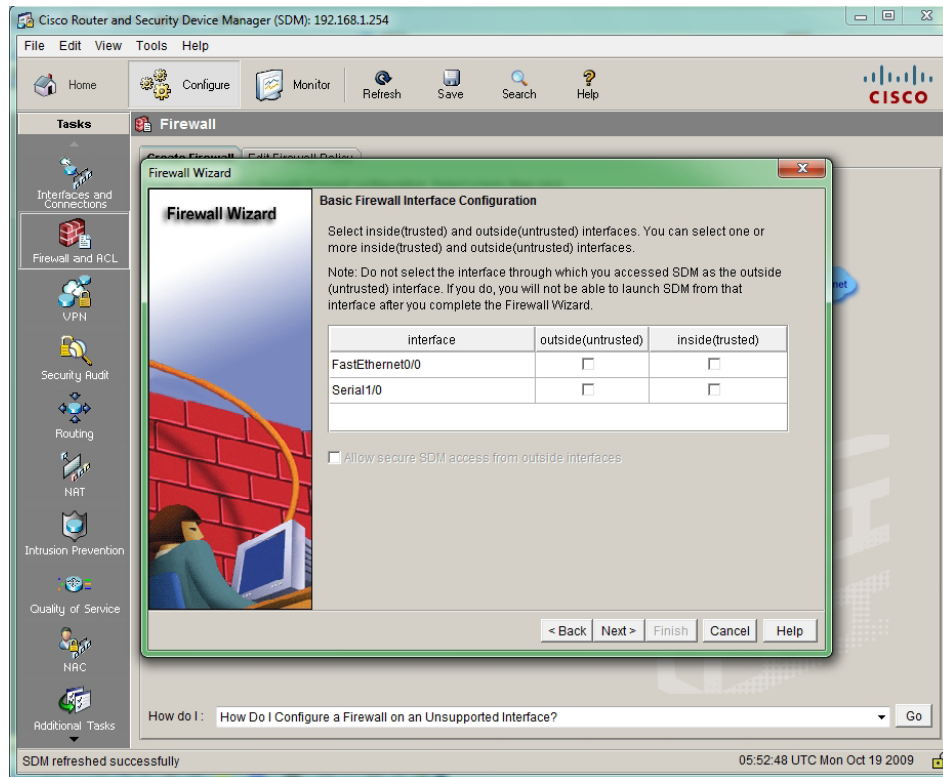


Figure 31 - Basic Firewall Wizard Interface Screen

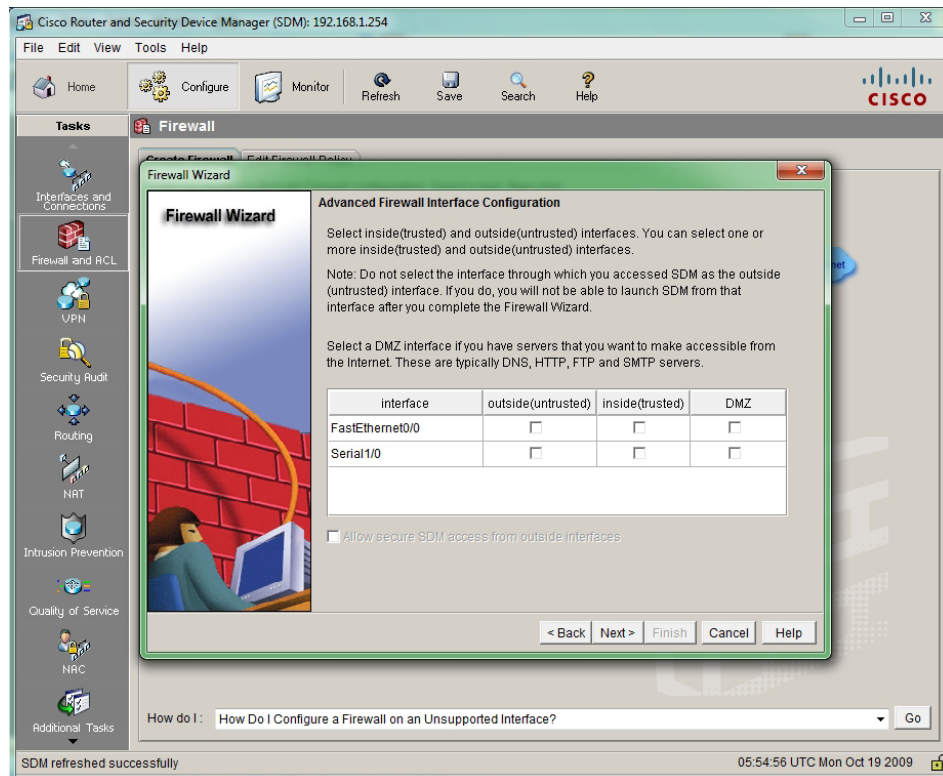


Figure 32 - Advanced Firewall Wizard Interface Screen

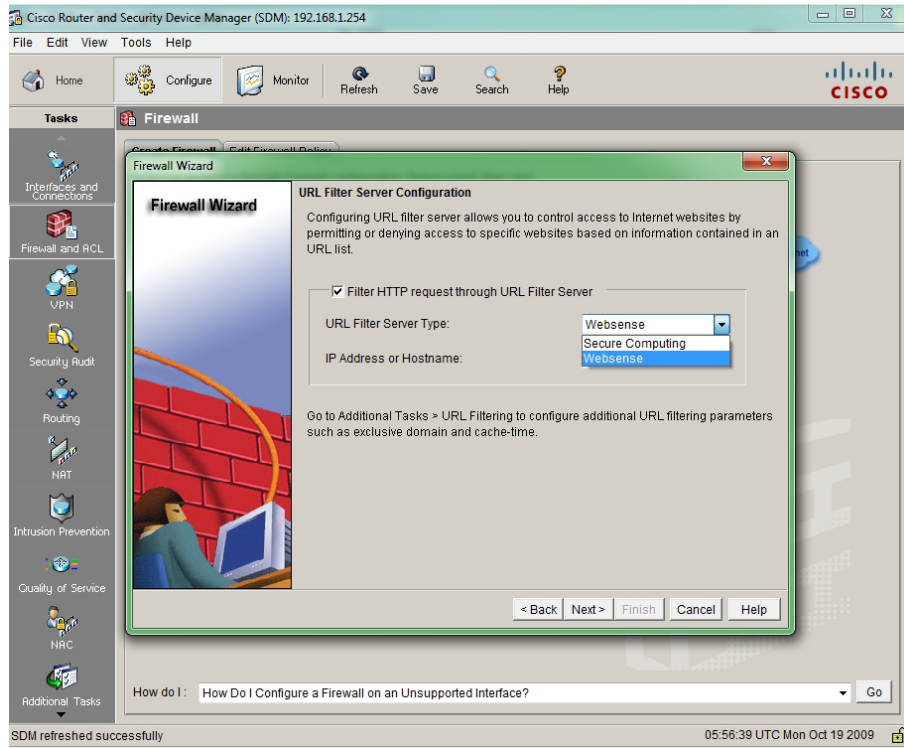


Figure 33 - Advanced Firewall Wizard URL Filter Screen

The second way of configuring a firewall through SDM is using the Edit Firewall Policy screen, as shown in Figure 34.

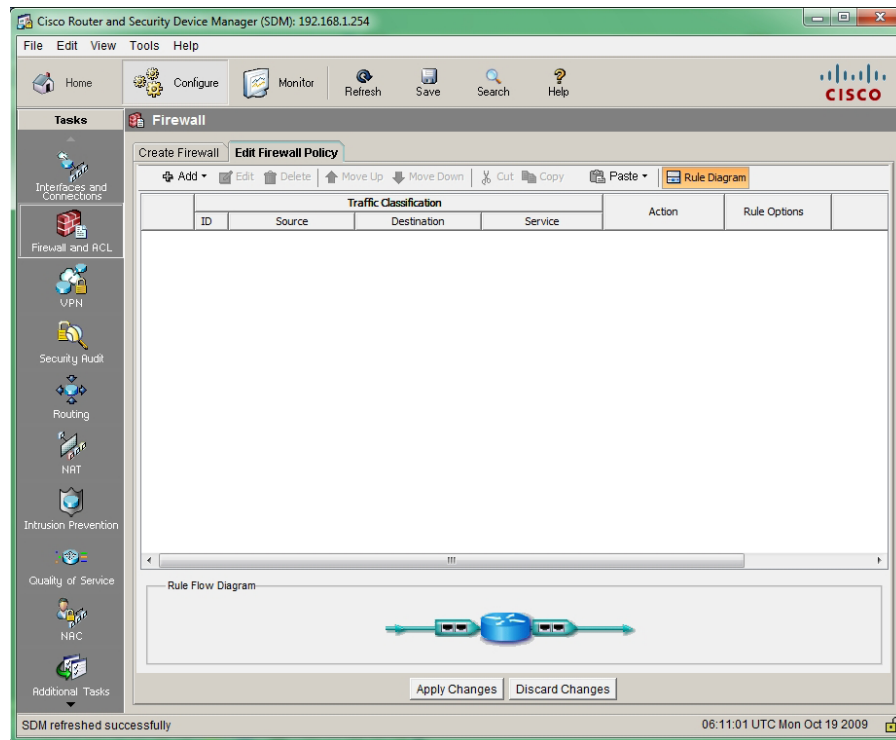


Figure 34 - SDM Edit Firewall Screen

## Domain 8 - Implement the Cisco IOS IPS feature set using SDM

The configuration of the IPS using SDM requires a signature file as well as the specific inside and outside interfaces. All configurations are done with SDM through a wizard. The basic screens which are required are shown in the following figures.

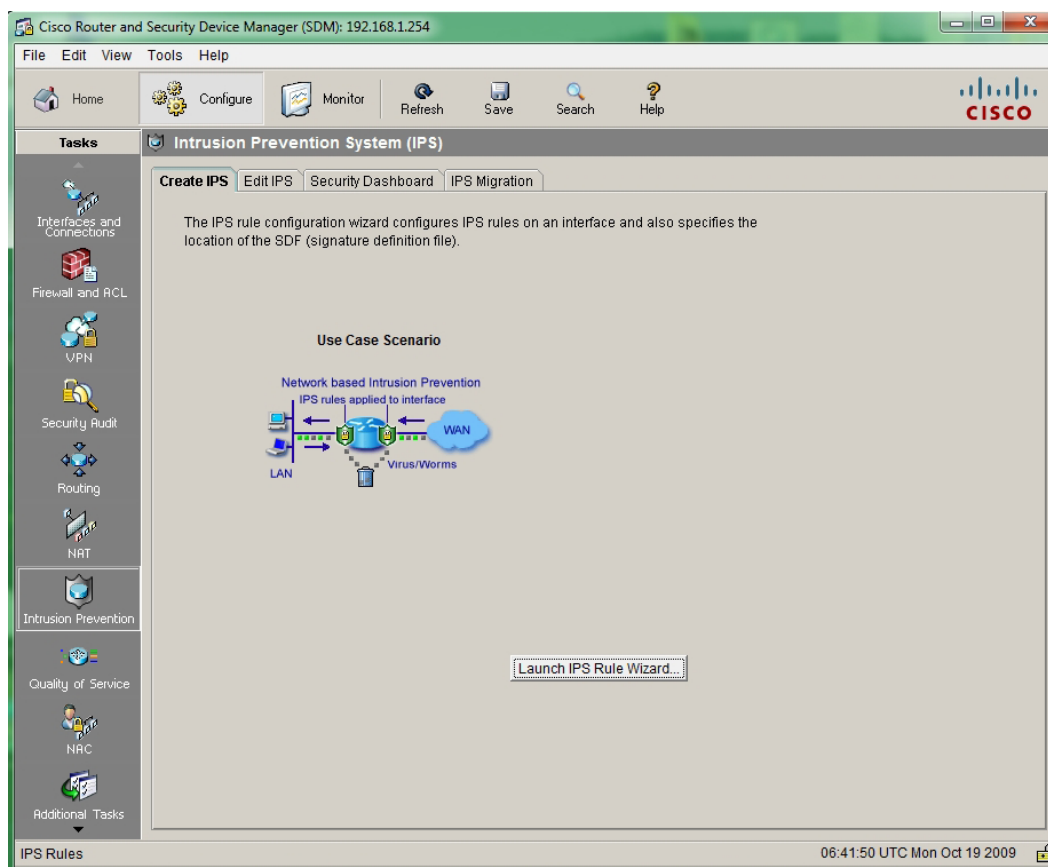


Figure 35 - Main IPS Screen

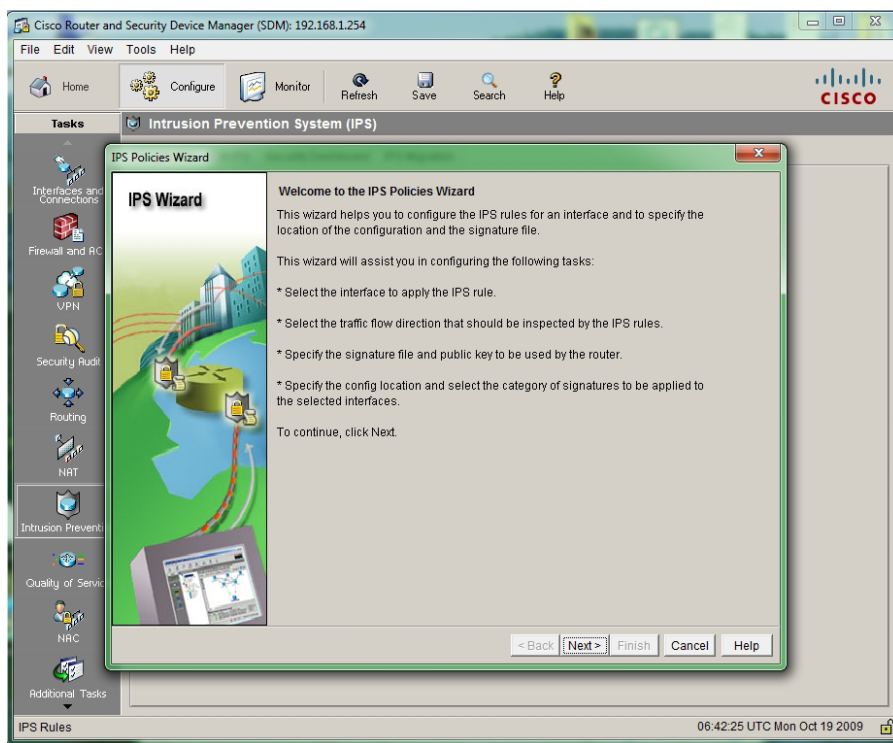


Figure 36 - IPS Wizard Screen

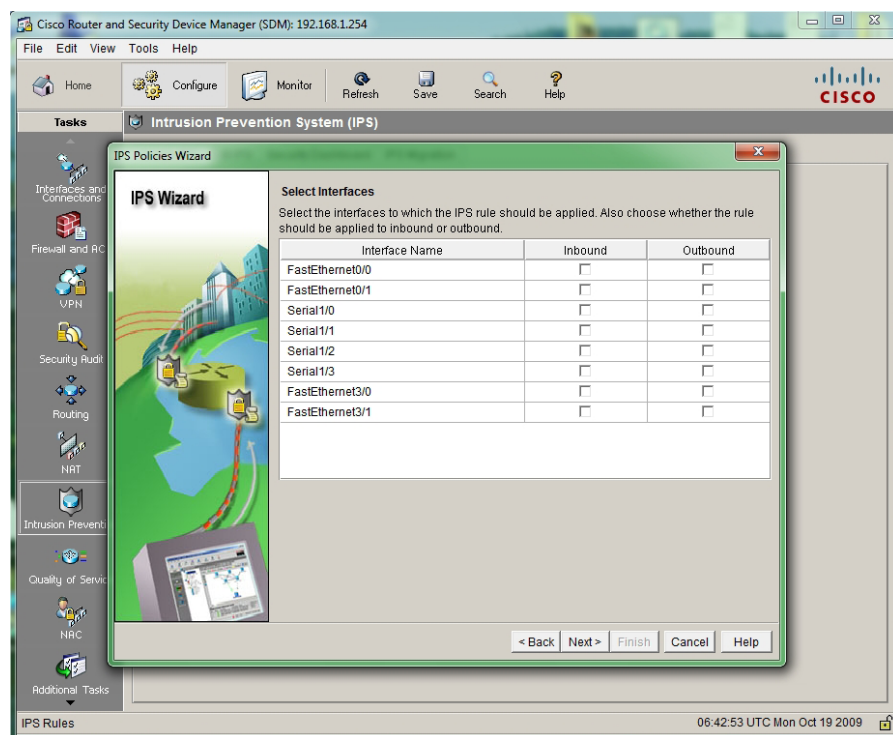


Figure 37 - IPS Interfaces Screen

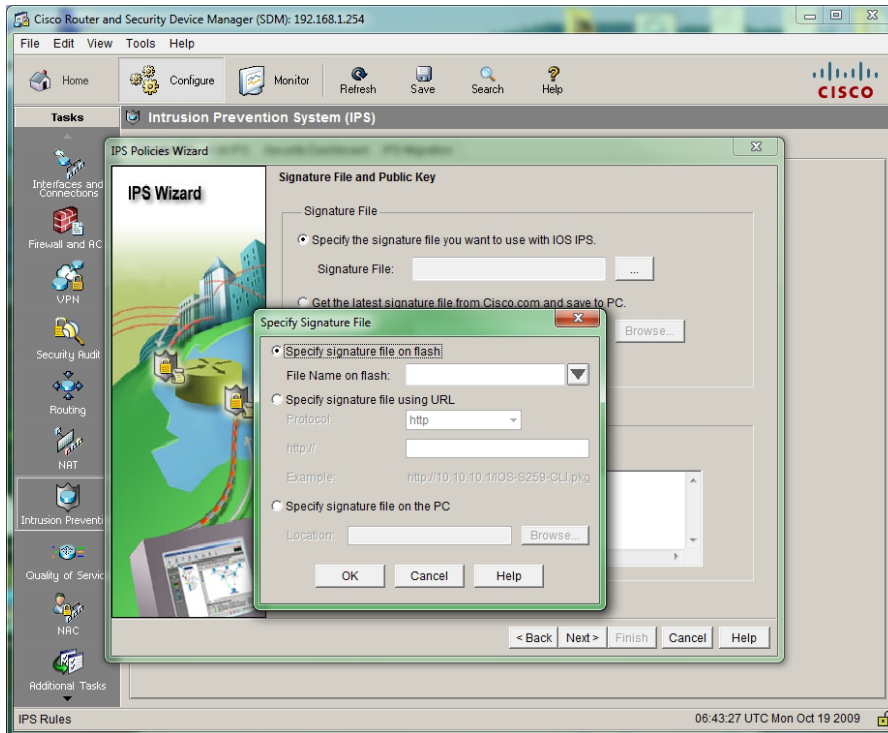


Figure 38 - Signature and Key Selection

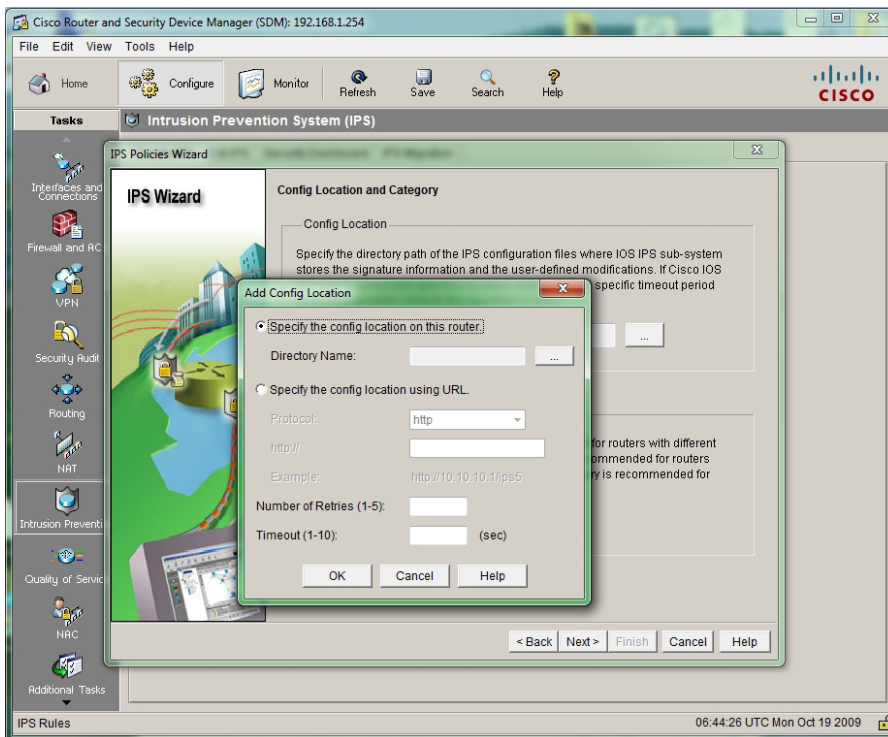


Figure 39 - IPS Configuration Selection

## Domain 9 - Implement site-to-site VPNs on Cisco Routers using SDM

A site-to-site VPN is a way to encrypt traffic between two private networks via an untrusted network. The following figure displays the network layout that is shown in the SDM configuration screens.

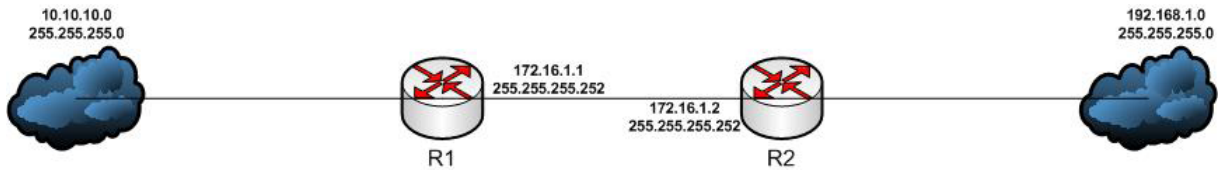


Figure 40 - Site-to-Site VPN Example Figure

In the following configuration screens, a site-to-site VPN is set up from R1 to R2.

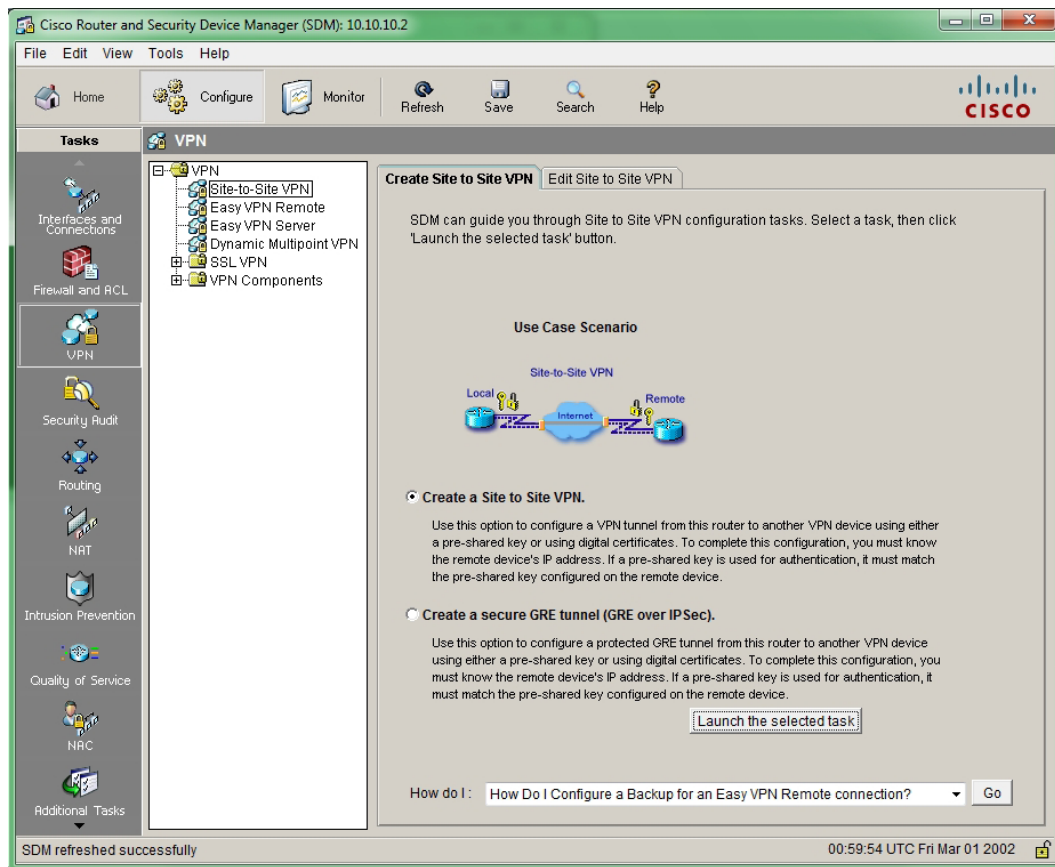


Figure 41 - Site-to-Site Main Screen



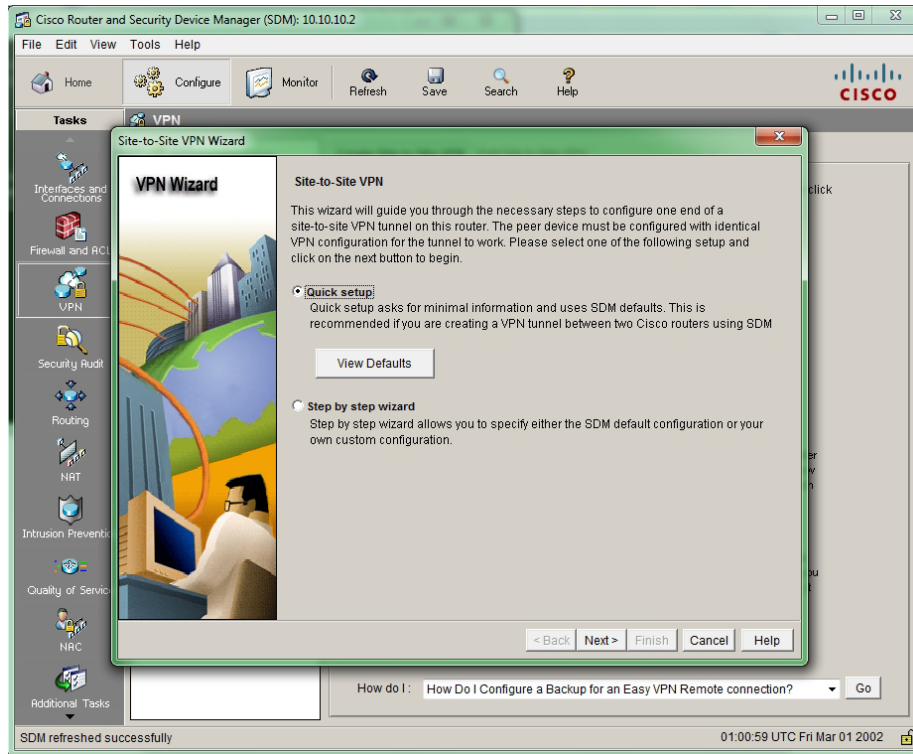


Figure 42 - Site-to-Site Setup Options

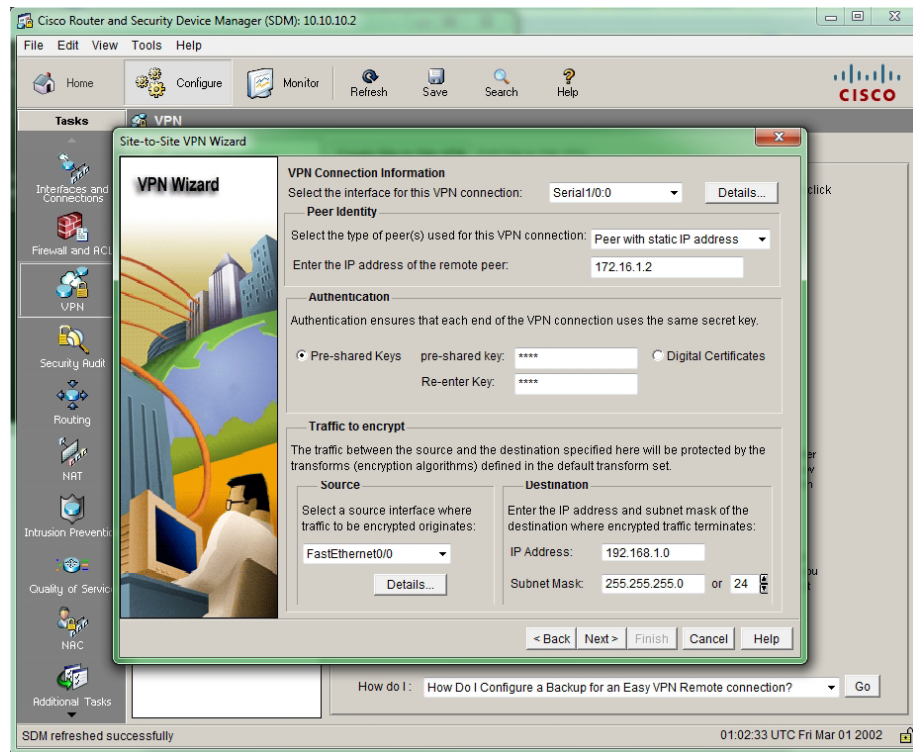


Figure 43 - Site-to-Site Quick Setup Parameters

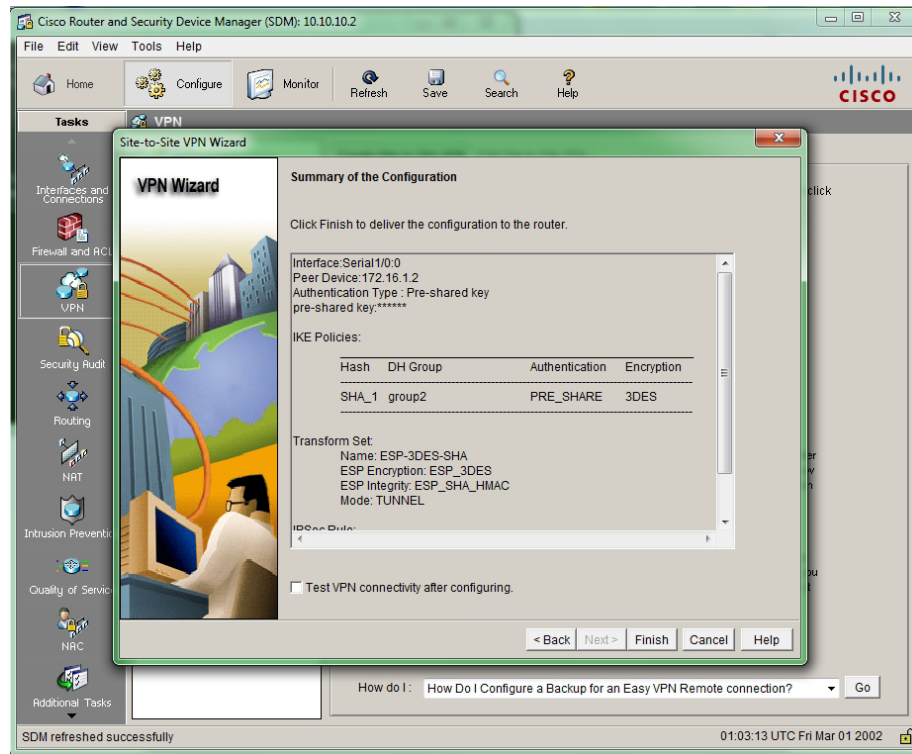


Figure 44 - Site-to-Site Quick Setup Summary

This simple SDM configuration automatically creates the CLI commands needed for this configuration. The following figure shows the CLI configuration as entered by SDM:

```

crypto isapolicy 1
  encr 3des
  authentication pre-share
  group2
  crypto isakmp key test address 172.16.1.2
  !
  crypto ipsec transform-set ESP-#DES-SHA esp-3des esp-sha-hmac
  !
  crypto map SDM_CMAP_11 ipsec-isakmp
  description Tunnel to 172.16.1.2
  set peer 172.16.1.2
  set transform-set ESP-3-DES-SHA
  match address 100
  !
interface FastEthernet0/0
  ip address 10.10.10.2 255.255.255.0
  duplex auto
  speed auto
  !
interface Serial 1/0/0
  ip address 172.16.1.1 255.255.255.252
  crypto map SDM_CMAP_1
  !
access-list 100 remark SDM_ACL Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255

```

Figure 45 - Site-to-Site CLI Configuration

## Practice Questions

### Chapter 1

1. Which of the following answers correctly shows a TCP handshake? Select the best answer.
  - A. SYN (Sequence Number = 1) SYN,ACK (Sequence Number = 0, Acknowledgement Number = 1) ACK (Sequence Number = 2, Acknowledgement Number = 0)
  - B. SYN (Sequence Number = 1) ACK (Sequence Number = 0, Acknowledgement Number = 2) SYN,ACK (Sequence Number = 2, Acknowledgement Number = 1)
  - C. SYN (Sequence Number = 1) SYN,ACK (Sequence Number = 0, Acknowledgement Number = 0) ACK (Sequence Number = 0, Acknowledgement Number = 2)
  - D. SYN (Sequence Number = 1) SYN,ACK (Sequence Number = 0, Acknowledgement Number = 2) ACK (Sequence Number = 2, Acknowledgement Number = 1)
2. What type of spoofing occurs when an attacker is not on the local subnet of the target? Select the best answer.
  - A. Blind Spoofing
  - B. Remote Spoofing
  - C. Local Spoofing
  - D. Non-Blind Spoofing

### Chapter 2

1. What command would be used to configure a reversible password to enter enable mode? Select the best answer.
  - A. router(config)#username username secret password
  - B. router(config)#enable secret password
  - C. router(config)#enable password password
  - D. router(config-line)#password password
2. What command would be used to create a separate privilege level 7 which would only allow the user to run basic show commands including the show running-config? Select the best answer.
  - A. router(config)#enable secret level 7 password router(config)#privilege exec level 7 show
  - B. router(config)#enable secret level 7 password router(config)#privilege exec level 7 show router(config)#privilege exec level 7 show running-config
  - C. router(config)#privilege exec level 7 show router(config)#privilege exec level 7 show running-config
  - D. router(config)#privilege exec level 7 show

## Chapter 3

1. What command would be used to configure reverse telnet authorization using TACACS+ by default? Select the best answer.
  - A. router(config)#aaa authorization reverse-access default group tacacs+
  - B. router(config)#aaa authorization reverse-access default tacacs+
  - C. router(config)#aaa authorization reverse-telnet default group tacacs+
  - D. router(config)#aaa authorization reverse-access com\_auth group tacacs+
2. What AAA command would be used to creating a connection to a TACACS+ server and is configured to open and close TCP sessions throughout each session? Select the best answer.
  - A. router(config)#tacacs-server host server-ip-address single-connection
  - B. router(config)#tacacs-server host server-ip-address
  - C. router(config)#tacacs-server server-ip-address single-connection
  - D. router(config)#tacacs-server server-ip-address

## Chapter 4

1. What would be the syntax for an extended access list to permit the 172.16.0.0/16 network to send telnet traffic to the 10.10.10.0/24 network using the first available ACL number? Select the best answer.
  - A. router(config)#access-list 100 permit tcp 172.16.0.0 0.0.255.255 10.10.10.0 0.0.0.255 eq telnet
  - B. router(config)#access-list 100 permit tcp 172.16.0.0 255.255.0.0 10.10.10.0 255.255.0.0 eq telnet
  - C. router(config)#access-list 1 permit tcp 172.16.0.0 0.0.255.255 10.10.10.0 0.0.0.255 eq telnet
  - D. router(config)#access-list 1 permit tcp 172.16.0.0 255.255.0.0 10.10.10.0 255.255.0.0 eq telnet
2. Referring to the exhibit, you are trying to configure an access-list to block spoofing attempts. Will the configuration in the exhibit provide a means to accomplish this? Select the best answer.
  - A. Yes, this configuration will correctly block traffic from the internal IP network from coming in the Internet port.
  - B. No, this configuration will not work correctly because the access-list is formatted incorrectly.
  - C. No, this configuration will not work because the access-group is not formatted correctly.
  - D. No, this configuration will not work correctly because the access-group is configured in the wrong direction.

## Chapter 5

1. Which two of the following are Cisco recommendations when planning for secure management and reporting? Select the best 2 answers.
  - A. Create a logging solution recommended by management.
  - B. Keep all logging levels set to their highest levels to retain the most information.
  - C. Keep all logging information in a central secure facility which can not be tampered with.
  - D. Develop a change management plan to deal with and document the changes being made to the network.

2. What versions of SNMP are supported on Cisco equipment? Select the best answer.
- A. Versions 1c, 2, and 3
  - B. Versions 1, 2, and 3
  - C. Versions 1, 2c, and 3c
  - D. Versions 1, 2c, and 3

## Chapter 6

1. What OSI layer relates to Layer 2? Select the best answer.
- A. Network
  - B. Transport
  - C. Data Link
  - D. Physical
2. What command would be needed to trust a port for DHCP snooping? Select the best answer.
- A. Nothing, all ports are trusted by default.
  - B. `switch(config-if)#ip dhcp trust snooping`
  - C. `switch(config-if)#ip dhcp trust`
  - D. `switch(config-if)ip dhcp snooping trust`
3. Which Cisco port security violation action is used to report when a violation occurs, and block all non-learned traffic? Select the best answer.
- A. Log
  - B. Restrict
  - C. Protect
  - D. Journal
4. Which Cisco port security violation action is used to report when a violation occurs, and block all learned and non-learned traffic? Select the best answer.
- A. Restrict
  - B. Protect
  - C. Shutdown
  - D. Learned

## Chapter 7

1. In application layer firewalls what layer of traffic is able to be filtered? Select the best answer.
- A. Layer 2, 3, 4 and 6
  - B. Layer 3, 4, 5 and 7
  - C. Layer 3, 4, 5 and 6
  - D. Layer 2, 3, 4, 5 and 7

2. On which ports does a stateful firewall operate? Select the best answer.
  - A. Layer 2, 3, and 4
  - B. Layer 3, 4 and 5
  - C. Layer 3, 4, and 6
  - D. Layer 2, 3, 4 and 6
  
3. Of the following, which are considered to be uses for application inspection firewalls? Select the best answer.
  - A. A primary means of defense.
  - B. Improve routing performance.
  - C. Defense against DoS attacks.
  - D. Most stringent control over security.
  
4. You are trying to setup an interface into the 'public' zone by using the 'zone-member security public' command but keep getting the '% Security zone name public not defined' message, why? Select the best answer.
  - A. The 'security zone public' command was not configured yet.
  - B. The 'zone security public' command was not configured yet.
  - C. The 'zone-member' command syntax was incorrect
  - D. The 'zone-member security public' command was not configured yet.

## Chapter 8

1. Which of the following IPS/IDS detection methods is used as a lure to attackers so they will waste time attacking an artificial target? Select the best answer.
  - A. Honey Pot
  - B. Signature-Based
  - C. Anomaly-Based
  - D. Policy-Based
  
2. What is the fundamental difference between an IPS and IDS? Select the best answer.
  - A. AN IPS is able to pro-actively protect you while an IDS does not.
  - B. An IDS is used to detect intrusions and the IPS are used to protect from those detected intrusions.
  - C. An IDS is able to pro-actively protect you while an IPS does not.
  - D. An IPS is used to detect intrusions and the IDS are used to protect from those detected intrusions.

3. What solution would be best if a large amount of your network traffic was encrypted and you were concerned with encrypted malicious traffic? Select the best answer.
- A. NIDS
  - B. HIPS
  - C. IPSD
  - D. NIPS
4. What type of signature looks for signs of extraordinary resource consumption and flags this behavior? Select the best answer.
- A. Exploit Signatures
  - B. String Signatures
  - C. Connection Signatures
  - D. DoS Signatures

## Chapter 9

1. Of the following algorithms which is one of the three algorithms used to make up a digital signature? Select the best answer.
- A. Rijndael Algorithm
  - B. Signature generation algorithm
  - C. Signature verification algorithm
  - D. Key verification algorithm
2. Of the following encryption types which is used in asymmetric encryption? Select the best answer.
- A. Diffie-Hellman
  - B. AES
  - C. Blowfish
  - D. DES
3. Which of the following is not considered to be a caveat of PKI? Select the best answer.
- A. User Private Key Stolen.
  - B. Server Private Key Stolen.
  - C. Client Public Key Stolen.
  - D. Certificate Authority (CA) Compromised.

# Answers & Explanations

## Chapter 1

### 1. Answers: D

Explanation A. Incorrect, the TCP flags are correct but the SEQ and ACK numbers are not.

Explanation B. Incorrect, The TCP flags are incorrect. The TCP handshake order is SYN, SYN-ACK, ACK.

Explanation C. Incorrect, the TCP flags are correct but the SEQ and ACK numbers are not.

**Explanation D.** Correct, this correctly shows both the TCP flag order and the SEQ and ACK numbers.

### 2. Answers: A

**Explanation A.** Correct, blind spoofing happens when an attacker launches a spoofing attack but is not on the local subnet.

Explanation B. Incorrect, while this answer is misleading this is not the correct answer. Blind spoofing is what happens when an attacker launches an attack and is not on the local subnet.

Explanation C. Incorrect, blind spoofing is what happens when an attacker launches an attack and is not on the local subnet.

Explanation D. Incorrect, Non-blind spoofing happens when an attacker launches an attack and IS on the local subnet.

## Chapter 2

### 1. Answers: C

Explanation A. Incorrect, this command would setup a local user with a password which utilizes MD5 but will not prompt when going into enable mode.

Explanation B. Incorrect, this is used to configure a password which would use MD5 and be prompted on entry to enable mode but MD5 is not reversible.

**Explanation C.** Correct, this command would be used. This question requires a little bit of thought because this command by itself would not use encryption however if used with service password-encryption it will use reversible encryption.

Explanation D. Incorrect, this command would utilize encryption if the service password-encryption command was also used.



## 2. Answers: B

Explanation A. Incorrect, these commands would correctly create a privilege level 7 and allow basic show commands but would not allow show running-config.

**Explanation B.** Correct, these commands would correctly create a privilege level 7, allow basic show commands and allow the show running-config command.

Explanation C. Incorrect, while these commands would properly set the privileges it would not be usable until a password was created for privilege level 7.

Explanation D. Incorrect, this command would correctly set privileges for basic show commands but would not allow the show running-config command. It would also not be usable until a password was created for privilege level 7.

## Chapter 3

### 1. Answers: A

**Explanation A.** Correct, this command would correctly enable AAA TACACS+ authentication when using reverse telnet.

Explanation B. Incorrect, this command is mostly correct. Before the 'tacacs+' keyword 'group' is required.

Explanation C. Incorrect, this command is almost correct except the correct command for reverse telnet is 'reverse-access' not 'reverse-telnet'.

Explanation D. Incorrect, this command is incorrect because it does not create a default method; this would be done by using the 'default' keyword instead of a list-name ('com\_auth').

### 2. Answers: B

Explanation A. Incorrect, this configuration would setup a connection to the TACACS+ server but it would maintain a connection to the server throughout the session.

**Explanation B.** Correct, this command would correctly setup a connection to the TACACS+ server and not setup a constant connection throughout the session.

Explanation C. Incorrect, this command does not have correct syntax. The host keyword is required after 'tacacs-server' for it to work correctly.

Explanation D. Incorrect, this command does not have correct syntax. The host keyword is required after 'tacacs-server' for it to work correctly.

## Chapter 4

### 1. Answers: A

**Explanation A.** Correct, this statement would correctly allow telnet traffic from the 172.16.0.0/16 network to the 10.10.10.0/24 network using the first available extended ACL number.

Explanation B. Incorrect, the general syntax is correct except that access-lists use wildcard masks.

Explanation C. Incorrect, this command syntax is correct but the first available extended access-list number is incorrect.

Explanation D. Incorrect, this command syntax is correct but the first available extended access-list number is incorrect and access-lists use wildcard masks.

### 2. Answers: D

Explanation A. Incorrect, this configuration will not work because the access-group command is configured in the wrong direction if it is to be applied on this interface.

Explanation B. Incorrect, the access-list command is formatted correctly.

Explanation C. Incorrect, the access-group command is formatted correctly.

**Explanation D.** Correct, in the exhibit either the interface needs to change or the direction needs to change for this configuration to work.

## Chapter 5

### 1. Answers: C, D

Explanation A. Incorrect, it is recommended that all levels of the team be consulted when recommending a logging solution.

Explanation B. Incorrect, if the highest level of logging is used it is easy for a problem to be missed inside the vast number of messages sent.

**Explanation C.** Correct, it is recommended that all logging information be sent to a secure central location which is used in case a device is tampered with.

**Explanation D.** Correct, it is recommended that a change management program be used to track all changes to a system. This is useful because this granular tracking provides vital data for troubleshooting and for reference information for future changes.

### 2. Answers: D

Explanation A. Incorrect, the supported versions are 1, 2c and 3.

Explanation B. Incorrect, the supported versions are 1, 2c and 3.

Explanation C. Incorrect, the supported versions are 1, 2c and 3.

**Explanation D.** Correct, these are the correct supported versions.

## Chapter 6

### 1. Answers: C

Explanation A. Incorrect, layer 2 associates with the data link OSI layer.

Explanation B. Incorrect, layer 2 associates with the data link OSI layer.

**Explanation C.** Correct, layer 2 associates with the data link OSI layer.

Explanation D. Incorrect, layer 2 associates with the data link OSI layer.

### 2. Answers: D

Explanation A. Incorrect, all ports are not trusted by default.

Explanation B. Incorrect, this is not the correct syntax.

Explanation C. Incorrect, this is not the correct syntax.

**Explanation D.** Correct, this command would correctly enable a port to be trusted for DHCP snooping.

### 3. Answers: B

Explanation A. Incorrect, the correct port security action is Restrict.

**Explanation B.** Correct, the restrict port security action is used to report violations is Restrict.

Explanation C. Incorrect, the correct port security action is Restrict.

Explanation D. Incorrect, the correct port security action is Restrict.

### 4. Answers: C

Explanation A. Incorrect, the correct port security action is Shutdown.

Explanation B. Incorrect, the correct port security action is Shutdown.

**Explanation C.** Correct, the correct port security action that will report and shutdown the port to all traffic is the Shutdown action.

Explanation D. Incorrect, the correct port security action is Shutdown.

## Chapter 7

### 1. Answers: B

Explanation A. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

**Explanation B.** Correct, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

Explanation C. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

Explanation D. Incorrect, an application layer firewall has the option of filtering on layers 3, 4, 5 and 7.

## 2. Answers: B

Explanation A. Incorrect, a stateful firewall operates on layers 3, 4, and 5.

**Explanation B.** Correct, a stateful firewall operates on layers 3, 4 and 5. This gives a stateful firewall the ability to monitor the state of the connections.

Explanation C. Incorrect, a stateful firewall operates on layers 3, 4 and 5.

Explanation D. Incorrect, a stateful firewall operates on layers 3, 4, and 5.

## 3. Answers: D

Explanation A. Incorrect, application inspection firewalls should be used as a secondary defense.

Explanation B. Incorrect, application inspection firewalls do not improve routing performance because they are processor intensive.

Explanation C. Incorrect, application inspection firewalls should not be used to defend Implement the Cisco IOS firewall feature set using SDM 32 against DoS attacks.

**Explanation D.** Correct, application inspection firewalls are considered to be the most stringent of all the firewalls.

## 4. Answers: B

Explanation A. Incorrect, the syntax of this command is incorrect. The correct syntax is 'zone security public'.

**Explanation B.** Correct, it is required that a zone be configured before a zone is assigned to an interface.

Explanation C. Incorrect, the 'zone-member' syntax is correct but a zone must be configured before a zone can be configured onto an interface.

Explanation D. Incorrect, the 'zone-member' command is correct for the interface but can't be configured before a zone is configured.

# Chapter 8

## 1. Answers: A

**Explanation A.** Correct, a honey pot is used as a distracter for attackers. This "honey pot" is then used as a sacrificial target.

Explanation B. Incorrect, a signature based attack does not utilize a lure for protection.

Explanation C. Incorrect, an Anomaly-based attack does not utilize a lure for protection.

Explanation D. Incorrect, a Policy-based attack does not utilize a lure for protection.

## 2. Answers: A

**Explanation A.** Correct, an IPS is a protection system that sits inline in the network and can proactively prevent attacks.

Explanation B. Incorrect, the IDS has the ability to tell IPS's to block traffic as well as other pieces of equipment. An IPS has the ability to block and detect by itself.

Explanation C. Incorrect, an IDS does not have the ability to proactively protect from an attack because it is not inline. It can however catch an attack shortly after it is launched.

Explanation D. Incorrect, the IPS is used to both detect and protect from attacks. The IDS can also detect attacks and alert several pieces of equipment to take action including an IPS.

## 3. Answers: B

Explanation A. Incorrect, a Network-based Intrusion Detection System is limited to traffic it can read if the traffic is encrypted to the host then this traffic would be invisible to the NIDS.

**Explanation B.** Correct, a Host-based Intrusion Protection System would have the ability to monitor this traffic because the encryption would be stripped off by the time it was read by the HIPS.

Explanation C. Incorrect, there is no such protection system.

Explanation D. Incorrect, a Network-based Intrusion Protection System is limited to traffic it can read if the traffic is encrypted to the host then this traffic would be invisible to the NIPS.

## 4. Answers: D

Explanation A. Incorrect, exploit signatures are used to match specific exploits.

Explanation B. Incorrect, string signatures look for a specific string inside a traffic stream.

Explanation C. Incorrect, connection signatures are programmed to watch for how certain protocols behave and look for abnormalities in this behavior.

**Explanation D.** Correct, DoS signatures look for a specific sign of DoS attacks. Since DoS attacks function to utilize the resources of piece of network equipment to a point where legitimate traffic can not get through, the way to look for this is through odd patterns in resource consumption.

# Chapter 9

## 1. Answers: C

Explanation A. Incorrect, Rijndael is the algorithm behind AES.

Explanation B. Incorrect, there is no such algorithm.

**Explanation C.** Correct, the Signature verification algorithm is one of the three algorithms generally used for digital signatures. The others are the key generation algorithm and the signing algorithm.

Explanation D. Incorrect, there is no such algorithm.

**2. Answers: A**

**Explanation A.** Correct, this encryption type is used for asymmetric encryption.

Explanation B. Incorrect, this encryption type is used for symmetric encryption.

Explanation C. Incorrect, this encryption type is used for symmetric encryption.

Explanation D. Incorrect, this encryption type is used for symmetric encryption.

**3. Answers: C**

Explanation A. Incorrect, if any private key is stolen then all information which used this key for security is vulnerable.

Explanation B. Incorrect, if any private key is stolen then all information which used this key for security is vulnerable.

**Explanation C.** Correct, there is no such a thing as a stolen public key because it is simply used to create a message to the key owner and is freely given to people to write secured traffic to the owner.

Explanation D. Incorrect, the CA being compromised questions the validity of any keys signed by this authority thus making all these keys vulnerable.