

Cisco SA500 Series Security Appliances

Small Business Pro Solution Demonstration



For
Small
Business



Table of Contents

Cisco SA500 Series Solution Overview	3
Cisco SA500 Security Gateway Demo Script	3
Demonstration Scripts Key	4
Preparing for the Demo	5
Bill of Materials	5
Getting Ready: The Night Before your Demonstration	6
Device Setup	6
Basic Demo	8
Getting Access to your Security Router	8
Managing User Accounts	10
Changing the Default Password	10
Configuring additional Administrator Accounts.....	11
Backup and Maintenance Tasks	12
Upgrading to a new Firmware.....	12
Backing up a working configuration.....	12
Configuring the Networking Interfaces	14
WAN Interface.....	14
LAN Interface	15
IPv6 Settings.....	16
Using the On-Box Help	18
Viewing System Information	19
Advanced Demo	20
Mobility	21
IPSec Virtual Private Network (VPN) Client Account Setup.....	21
OPTIONAL: SSL VPN & Client Portal Setup	23
Site-to-Site Virtual Private Network (VPN) Setup for Remote Office Locations.....	24
Firewall	27
Content Filtering	29
Filter URLs.....	29
DMZ Setup	31
Unified Threat Management	35
Intrusion Prevention System	35
Web Threat Protection (Cisco ProtectLink Gateway or Cisco Protectlink Web Services)	35
OPTIONAL: Email Protection (Cisco ProtectLink Gateway Service only).....	37
OPTIONAL: Endpoint Protection (Cisco ProtectLink Endpoint Service)	38

Cisco SA500 Series Solution Overview

The Cisco SA500 Series Security Appliances, part of the Cisco Small Business Pro Series, are comprehensive gateway security solutions that combine firewall, VPN, and optional intrusion prevention and web and email security capabilities, helping you feel confident that your business is protected and resilient. These easy-to-use security appliances let you control access to network resources, enabling you to protect business data and maximize network uptime. The Cisco SA500 Series also helps increase employee productivity by controlling web access, spam emails, phishing attacks, unauthorized intrusions, and other emerging threats, as well as by freeing IT resources from virus eradication and system cleanup activities. With the Cisco SA500 Series, you can safely deploy new business applications without opening up security holes. Mobile employees and business partners can also securely connect to your network over the Internet using IP Security (IPsec) or Secure Sockets Layer (SSL) VPN services. With a Cisco SA500 Series solution protecting your network, you can focus on growing your business without worrying about the latest security threats.

Cisco SA500 Security Gateway Demo Script

This Demonstration Script is centred on the SA500 Series of Security Appliances – their business grade security, advanced networking abilities and ease of use. The SA500 Series makes it easy for Small Businesses to build a secure network, manage it or expand an existing one, with or without a dedicated IT staff.

This document gives you the means to become more comfortable with the SA500 Series, and demonstrate its many benefits in sales and training events.

There are 2 types of demonstrations in this document – Basic and Advanced.

The *Basic* demo gives instructions on how to demonstrate the Management interface, while keying in on feature highlights. The *Advanced* demo gives instructions on how to demonstrate more advanced security features, such a remote worker accessing the local network through a VPN tunnel, protecting the small business network from outside threats using Cisco ProtectLink Gateway and Web Services, and the use of integrated Intrusion Prevention System (IPS).

All through the demonstration, we focus on the following items:

- Intuitive Graphical User Interface (GUI)
- Ease of Configuration
- Integration of security features to provide an all-in-one solution:
 - Integrated IPS in the SA500
 - Cisco Protectlink Gateway Service (Anti-virus, Web Threat Protection, Email Protection and SPAM Filtering)

- Cisco Protectlink Endpoint Service (anti-virus, URL filtering and POP3 SPAM filtering at the desktop and server level)
 - Cisco Small Business Routers and the Cisco ProtectLink Web Services are designed for the specific needs of small.
 - Advanced Feature set compared to similar products (shown in Advanced Demo)
-

Key Messages

- Protect the Small Business network by monitoring traffic that traverses the router for malicious activity and threats
 - Protect the WAN edge with web threat protection and email filtering services
 - Protect the endpoints with anti-virus, anti-spam and URL filtering software
 - Generates reports based on attack and threat activity
 - Endpoint Service can block or limit employee access to certain web sites, and P-2-P or social networking sites that leading to increased productivity.
-

For additional information, please reference the Administration Guide and Quick Start Guide available at: www.cisco.com/go/sa500

Demonstration Scripts Key

This demo provides a step-by-step guide to configuring various items in the SA500.

The SA520W is referenced in this demo, however you may use any other device in the SA500 series, such as SA520, SA520W or SA540.

We use the following notations:

STEP 1. Numbered instructions must be carried out in the order shown.

- Bulleted features in each script can be selected individually for alternate views or testing.



Note Instructions worth noting!

Preparing for the Demo

Bill of Materials

The **Basic** demo requires the following devices:

- SA500 appliance – SA520, SA520W or SA540
- Power Cord
- Ethernet Cable
- 1 PC with any web browser installed (Internet Explorer, Firefox, Safari or Chrome)
- OPTIONAL – an internet connection via a DSL router or Cable modem.

The **Advanced** demo is more complex and gives a more realistic snapshot of a live network, with multiple devices communicating securely, and incoming threats are blocked. This set of demonstrations requires an additional PC and a router for connecting to the Internet. The following devices are required:

- Cisco 300 Series Switch – SG300-10P or SG300-28MP
- Power Cord
- 3 Ethernet Cables
- 2 PCs:
 - Management PC with any web browser installed
 - 1 PC with the following:
 - Windows OS – either XP or earlier
 - QuickVPN software installed - to demonstrate Remote VPN and DMZ
- 1 PC or NSS32x to demonstrate DMZ
- RV120W or another SA500 – to demonstrate site-to-site VPN



Note You can show the Advanced demos within the Basic form, by simply explaining the solution you are configuring and walking through the configuration process

Getting Ready: The Night Before your Demonstration

1. Make you have all the necessary items on the Bill of Materials; per the scenario you will demonstrate.
2. Ensure that the web browser that you will be using is communicating effectively with your security router.
3. Download the latest firmware version and store it on your PC, or on a USB key. New firmware for the SA500 Series Security Appliances at: www.cisco.com/go/sa500software
4. Check the deployment scenario of the Service provider in the site in which you will be demonstrating SA500. Verify that:
 - SA500 will get an IP address from the WAN network
 - A login is required (PPPoE, L2TP or PPTP connections). If so – get these credentials: username, password and IP address
5. The SA500 allocates an IP address to your PC, so that you can communicate with the SA500, however you should also familiarize yourself with how to change the IP address on your PC, in case you will need it.
 - The SA500 LAN IP address is preconfigured to 192.168.75.1, so you need to ensure that your PC has allocated an IP address in the 192.168.75.0 subnet (for example: 192.168.75.25)
6. Reset the SA500 to its Factory Defaults, to show a clean, out-of-the-box configuration scenario.
 - To do this, insert a paper clip into the reset Button on the Front Panel, and press and hold it for 10 seconds. Or, enter the SA500 management page, and navigate to **Administration > Firmware and Configuration > Network**, go to **Backup and Restore Settings** paragraph and click on the **Default** button.
7. It is advised to have an Internet Access device at the premise to show connectivity to the internet
8. If you plan to demonstrate the optional ProtectLink scenarios, ensure that you have the licenses at hand and endpoint software installed on laptops that you will be using
9. Practice the demonstration scenarios a few times, so you become fluent with the demonstration actions and items to stress and point out to your audience.

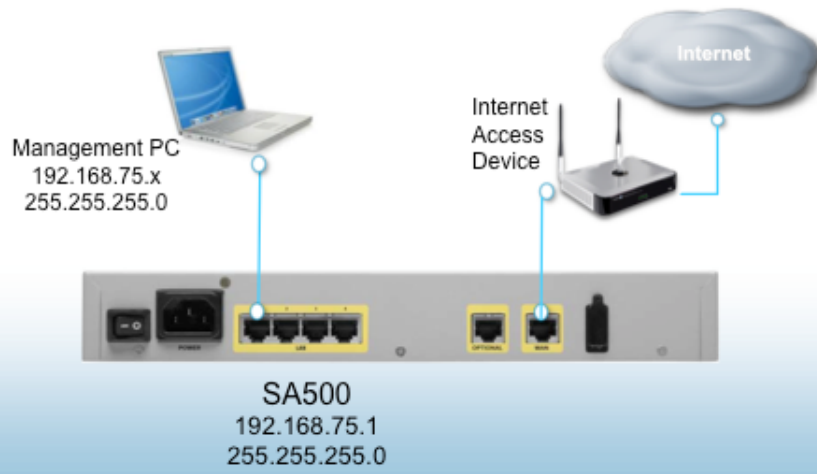
Device Setup

- STEP 1.** Plug the power cord to the SA500 (power port is located at the back side of the router).
- STEP 2.** Connect an Ethernet Cable from the Ethernet port of your management PC to Port 1 of the SA500's Ethernet Port. The lights on the front panel will light up to indicate that the Port is operational, and specify the speed of the link.
- Port 1 is given as an example, but you can alternatively connect the cable to any other LAN port.
- STEP 3.** Connect an Ethernet cable from the LAN port of your Internet Access device to the WAN port of the SA500.

Your network Topology should look like this:

Basic Setup

For
Small
Business
Cisco



Basic Demo

This set of demonstrations centers on the basic configuration of the SA500 Routers. It is configured to operate out-of-the-box; however in many cases in real-world deployments, additional settings are required.

Throughout your demonstration, highlight and showcase the intuitive management interface, its ease-of-use and aesthetics. This interface is common through not only the SA500 routers, but also across many other SBTG products.

This section covers the following scenarios:

- Gaining Access to the SA500
- Configuring additional User Accounts
- Backup and Maintenance Tasks Upgrading to a new Firmware and Backing up a working configuration
- Configuring the Management Interface, IPv4 and IPv6
- Using the on-box Help
- Viewing System Information

Getting Access to your Security Router

The Cisco SA520W Router is accessible via the following options:

- Web-based configuration GUI
- Cisco Configuration Assistant (CCA)
- Menu based Console
- Remote Management using SNMP

Here we demonstrate access through the web-based GUI, which is both aesthetically pleasing to the user, and intuitive in its functions. Highlight this, as you go about your demonstration

STEP 1. The SA500 Series router is preconfigured for IP address 192.168.75.1 on its LAN side.


STEP 2. A DHCP server is also built in; therefore your PC will receive an IP address in the 192.168.75.0 subnet, with subnet mask of 255.255.255.0.

Verify that your PC has received an IP address from the router, in the 192.168.75.0 subnet

STEP 3. Start a Web Browser, and enter the router's IP address in the address bar: <https://192.168.75.1>

STEP 4. When the login page appears, enter the user name and password; then click Login.

The default user name is **cisco**. The default password is **cisco**. Passwords are case sensitive.



The screenshot shows the login interface for the Cisco Security Appliance Configuration Utility. The page has a dark blue header with the Cisco logo and the text "Small Business Pro Security Appliance Configuration Utility 1.0.15". On the right side, there are two input fields: "Username:" with the value "cisco" and "Password:" with masked characters "*****". Below these fields is a "Log In" button and a link for "Problems logging in?".

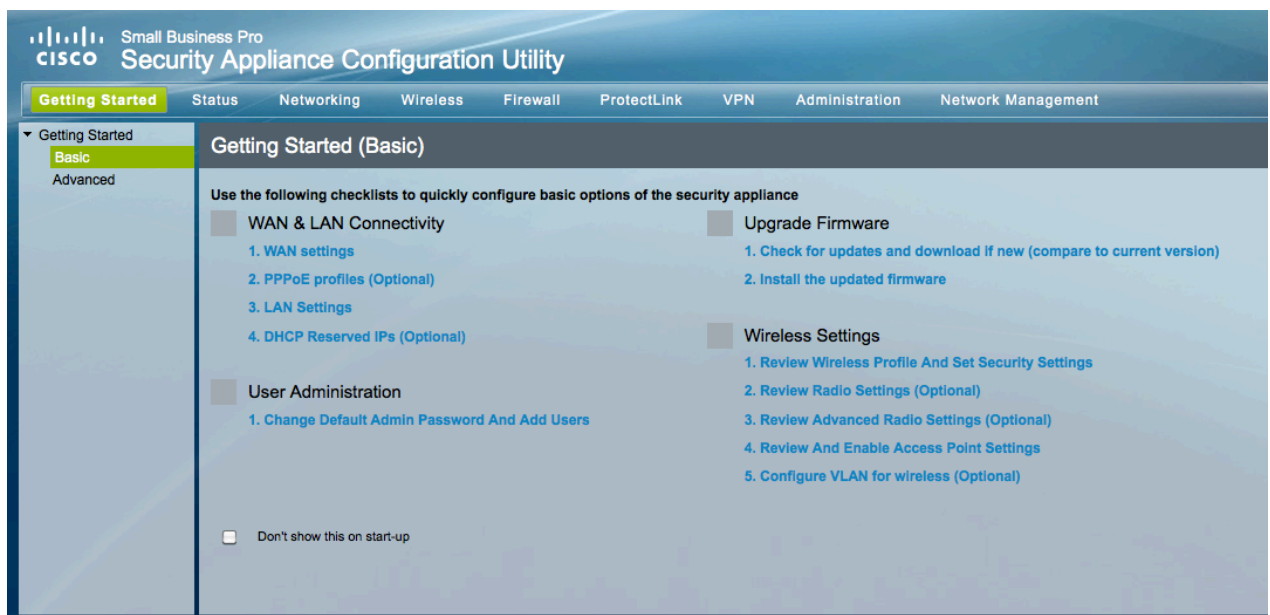
STEP 5. When the Security Alert appears, accept or install the certificate:

- **Internet Explorer:** Click **Yes** to proceed, or click **View Certificate** for details. On the Certificate page, click **Install the Certificate**. Follow the instructions in the Wizard to complete the installation.
- **Firefox:** Click the link to add an exception. Click the **Add Exception** button. Click **Get Certificate**, and then click **Confirm Security Exception**.
- **Safari:** Click **Continue** to proceed, or click **Show Certificate**. On the Certificate page, click **Install the Certificate**. Follow the instructions in the Wizard to complete the installation.

STEP 6. Once logged in, the **Getting Started (Basic)** page appears.

You can use the Basic page to access common configuration scenarios, such as WAN and LAN settings, Firmware upgrade and Administration tasks, all of which will be demonstrated here. The more Advanced configuration options will be demonstrated in the Advanced section of this demonstration. These quick-links are available under **Getting Started > Advanced**.

STEP 7. The SA500 Series GUI comes with links on the top of the page to various topics of configuration. This menu bar appears on every screen for easy and quick navigation. Within each link, you will find links to more specific configurations. We will access these throughout the Demo, so you become familiar with the possibilities



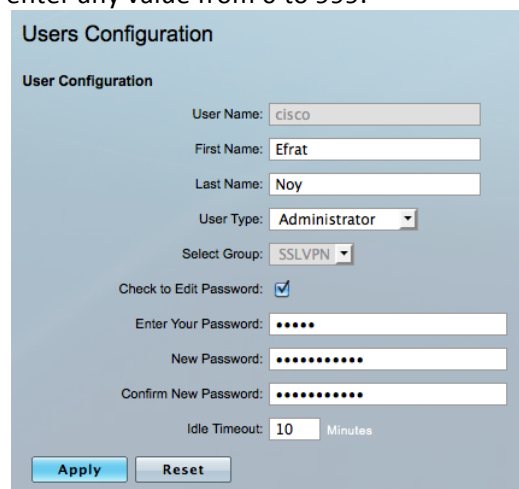
Managing User Accounts

After you have logged into the system, it is advisable to change the default Administrator password to prevent unauthorized access by malicious users who can damage your settings.

Alternatively, it is wise to add trusted administrative profiles, to ease the scheduling of IT staff.

Changing the Default Password

- STEP 1.** In the **User Administration** section of the Getting Started (Basic) page, click **Change Default Admin Password And Add Users**
- STEP 2.** You will see 2 default users, an **Administrator**, with configuration abilities (read-write access) and a **Guest** user, with only reading abilities.
- STEP 3.** To change the default password, click the button in the **Edit** column of the first row of the table. The **User Configuration** page will appear, displaying the default information.
- STEP 4.** To Add a new User, Select the **“Add”** button beneath the list.
- STEP 5.** Enter the following information:
 - User Name:** Enter a unique identifier for the user. It can include any alphanumeric characters, but make it one that you can easily remember.
 - First Name:** Enter your first name
 - Last Name:** Enter your last name
 - User Type:** this is not configurable
 - Check the **Check to Edit Password box**. This will enable the password fields at the bottom
 - Check this box to enable the password fields
 - Enter Your Password:** Enter the current password (Reminder: the default password for this new security appliance is **cisco**)
 - New Password:** Enter a password that contains alphanumeric, “—” or “_” Characters
 - Confirm Password:** Enter the selected password again.
 - Idle Timeout:** Enter the time in minutes that the user can be inactive before the login expires. You may enter any value from 0 to 999.



The screenshot shows the 'Users Configuration' page. It contains the following fields and controls:

- User Name:
- First Name:
- Last Name:
- User Type:
- Select Group:
- Check to Edit Password:
- Enter Your Password:
- New Password:
- Confirm New Password:
- Idle Timeout: Minutes
- Buttons:

- STEP 6.** Click **Apply** to save your settings

Configuring additional Administrator Accounts

STEP 1. Follow steps 1-2 of Scenario 1 above.

STEP 2. To add a new user, click the **Add** button. The **User Configuration** page will appear. Enter the following information:

User Name: Enter a unique identifier for the user. It can include any alphanumeric characters, but make it one that you can easily remember.

First Name: Enter your first name

Last Name: Enter your last name

User Type: select one of the following options:

- **Administrator:** for Read-Write privileges
- **Guest:** for Read-only privileges

Select Group: this is not configurable

Password: Enter a password that contains alphanumeric, “—” or “_” Characters

Confirm Password: Enter the selected password again.

Idle Timeout: Enter the time in minutes that the user can be inactive before the login expires. You may enter any value from 0 to 999.

Users Configuration

User Configuration

User Name: Efrat-Noy

First Name: Efrat

Last Name: Noy

User Type: Administrator

Select Group: SSLVPN

Password:

Confirm Password:

Idle Timeout: 15 Minutes

Apply **Reset**

STEP 3. Click **Apply** to save your settings. This will return you to the list of users capable to log in to the system.

Notice that the new user entered has been added successfully.

This will be indicated by a Success message at the top of the page.

Users

List of Users

<input type="checkbox"/>	User Name	Group	Type	Authentication Domain	Login Policy	Edit	Edit User Policies		
							Login	By Browser	By IP
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Enabled (LAN only)				
<input type="checkbox"/>	rmon1	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)				
<input type="checkbox"/>	rmon2	SSLVPN	Administrator	Local User Database	Enabled (LAN and WAN)				
<input type="checkbox"/>	guest1	SSLVPN	Guest	Local User Database	Enabled (LAN and WAN)				
<input type="checkbox"/>	suser1	SSLVPN	SSL VPN User	Local User Database	Enabled (LAN and WAN)				

Add... **Delete**

Backup and Maintenance Tasks

Upgrading to a new Firmware

Before doing any other tasks, you should upgrade your firmware to ensure that you are using the latest version. You can upgrade from a file stored on your computer, your network, or a USB key.



Note It is advisable to periodically check for new updates to your SA500 Series Router, as fixes are being uncovered and fixed.

New firmware for the SA500 Series Security Appliances at:

<http://www.cisco.com/go/sa500software>

- STEP 1.** From the **Getting Started** page, in the **Basic** tab, Click **Check for Updates and Download New Software**. This will direct you to cisco.com where the updated Firmware drops are stored. Download the latest software and store it on your PC, or on a portable USB key.
- STEP 2.** From the **Getting Started** page, in the **Basic** tab, Click **Install the Updated Firmware**. This will direct you to **Firmware and Configuration** page. Alternatively, you can reach this page through **Administration** tab, under **Firmware & Configuration > Network**.
- STEP 3.** In the **Software Upgrade** section, Click on **Browse**. This will open up a window from which you will select the file you have downloaded in Step 1.
- STEP 4.** Click on **Upload**. This will upload the new software onto the router and reboot it. Clicking **Upload & Factory Reset** will upload the new software, but will reset the settings to default. This operation will require reconfiguring the router.



Note Wait while the firmware is upgraded.

1. Do NOT close the browser window
2. Do NOT go online.
3. Do NOT turn off or power-cycle the router
4. Do NOT shutdown the computer.

The router will take several minutes to complete the upgrade. While the upgrade is in progress, the Test LED on the front panel of the router is lit.

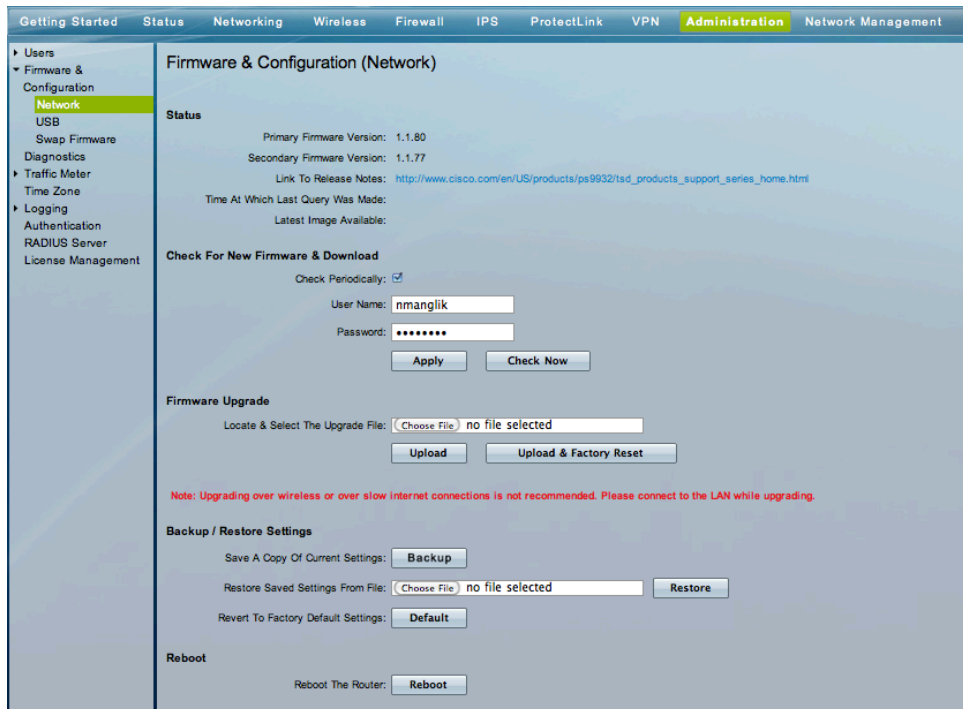
When the upgrade is complete, the router automatically restarts

Backing up a working configuration

It is advisable to back up your working configuration to protect your work from sudden power failures. Moreover, if you make changes that you want to abandon, you can easily revert back to a saved configuration.

Show with few simple steps, how you can back up a working configuration to your local hard-drive, and save it back to the router when needed.

- STEP 1. In the **Administration** menu bar, go to **Firmware & Configuration > Network** page through the navigation pane in the left-hand side of the GUI. The **Firmware & Configuration (Network)** page will appear.
- STEP 2. In **Backup / Restore Settings** section, click on **Backup** next to **Save a copy of current settings**.
- STEP 3. Read the warning that appears, and then click **OK**. When the Download window appears, click **Save**, and then choose a location where you want to save the file. Name the file such that you will remember its attributes, like adding the date appended to it. For example: **sa520w-20100923.cfg**
- STEP 4. To revert back to a working configuration, simply click **Browse** next to **Restore saved settings from file**. This will open a browsing window, where you will select the configuration file to restore.



Configuring the Networking Interfaces

In a basic deployment for a small business, the security appliance enables communication between the user devices on the Small Business network, and also allows them to access the Internet.

The SA500 devices already comes with default settings that allow it to be operational right out of the box. However, those settings might not fit various Internet Service Providers' deployment scenarios, and the router might need additional configuration to fit the local deployment technology.

WAN Interface

With the default settings, the SA500 gets its WAN address dynamically from the ISP. This is the case of most deployments, however if your ISP requires you to provide a login, you would need to change the WAN configuration to get access to the Internet.



Note Check the deployment scenario of the site in which you will be demonstrating this device, and get the appropriate details from that service provider, or site owner

- STEP 1.** From the **Getting Started** page, in the **Basic** tab, Click **WAN Settings**. This will lead you to **IPv4 WAN Configuration**. Alternatively, you can reach this page through **Administration > WAN > IPv4 Config**
- STEP 2.** If your ISP grants you a dynamic IP Address, you will need to leave the **Internet (IP) Address** field at **"Get Dynamically for ISP"**. Click **Apply** to save changes.
- STEP 3.** If your ISP requires a login, click the **Internet Connection Requires a Login** box under **ISP Configuration**, at the top of the page.
This will enable you to write into the fields under **ISP Connection Type**. Insert the correct values into the fields as instructed by your ISP, and click **Apply** to save your changes.
SP Connection Type: Choose the connection type, as specified by your service provider: PPTP, PPPoE, or L2TP. Then complete all fields that are highlighted with white backgrounds.
Profile Name: Choose a PPPoE Profile.



Note You can create a PPPoE profile by going into **Networking > WAN > PPPoE Profiles**, and clicking **Add**. This will lead you to the **PPPoE Profiles Page**. Complete the fields as instructed by your ISP.

The screenshot shows the Cisco ASA500 configuration interface. The top navigation bar includes 'Getting Started', 'Status', 'Networking' (highlighted), 'Wireless', 'Firewall', 'IPS', and 'ProtectLink'. The left sidebar shows a tree view under 'WAN' with 'WAN Status', 'IPv4 Config', 'PPPoE Profiles' (highlighted), and 'IP Alias'. The main content area is titled 'PPPoE Profiles' and contains the 'PPPoE Profile Configuration' section. Fields include: Profile Name: DSL1; User Name: Efrat; Password: masked with dots; Authentication Type: Auto-negotiate (dropdown); Connectivity Type: Keep Connected (dropdown); Idle Time: (Minutes) (input field). At the bottom are 'Apply' and 'Reset' buttons.

User Name: The user name that is required to log

Password: The password that is required to log

Secret(Optional): Enter the secret phrase to log into the server (if applicable)

Connectivity Type: Choose one of the following options:

- **Keep Connected:** The connection is always on, regardless of the level of activity. Choose this option if you pay a flat fee for your Internet service.
- **Idle Time:** The security appliance disconnects from the Internet after a specified period of inactivity (Idle Time). If you choose this option, also enter the **Idle Time** in minutes. Choose this option if your ISP fees are based on the time that you spend online

My IP Address: Enter the IP address assigned to you by the ISP

Server IP Address: Enter the IP address of the PPTP, PPPoE, or other server

STEP 4. If the WAN connection is brought up successfully, try to access a popular web site, like <http://www.cisco.com> or www.google.com.

STEP 5. To check your WAN connection, go to the **WAN Status** page under **Networking > WAN** menu. This will test your WAN connection and give you indication of whether your connection is up and running.

A successful WAN connection will show **WAN State** to be **UP**



Note If you are having trouble with your WAN connection, refer to the Troubleshooting guide in the **SA500 Administration Guide**, available at www.cisco.com/go/sa500

LAN Interface

With the default settings, all devices on the LAN receive their IP addresses dynamically from the security appliance through DHCP. The IP addresses allocated will be on the 192.168.75.0 subnet, with a default gateway of 192.168.75.1, which is the LAN IP address of the router.

Here we will show how to change the LAN subnet of your network, and how to manage the allocated DHCP addresses.

- STEP 1.** From the **Getting Started (Basic)** page, access the **LAN Settings** link under **WAN & LAN Connectivity**. Alternatively you can reach this page by going to the **Networking** tab, choose the **LAN > IPv4 Config**
- STEP 2.** Under **LAN TCP/IP Setup**, you will see the default value of the SA500 LAN configuration: IP address: 192.168.75.1 with a 24-bit subnet mask (255.255.255.0).
Change the **IP Address** to 10.10.10.1
Notice that this operation will require you to change the range of IP addresses being allocated. Follow on to the next step to do this.
- STEP 3.** Under **DHCP**, leave **DHCP Mode** as **DHCP Server**.
Change the **Starting IP Address** to 10.10.10.100 and **Ending IP Address** to 10.10.10.254.
This configuration will allow up to 155 users on your network.
- STEP 4.** For demo purposes, we want to ensure connectivity between the SA500 and your PC, so do not apply these changes:
Click **Reset** to disregard this configuration.

In some network configurations, the network administrator would want to utilize another DHCP server on the network; for example, if a DHCP server already exists on the network, or if the ISP gives out IP addresses to devices on the Small Business network.



Note Check with the network administrator of the location in which you will be demonstrating what the requested configuration might be.

- STEP 1.** From the **Getting Started (Basic)** page, access the **LAN Settings** link under **WAN & LAN Connectivity**. Alternatively you can reach this page by going to the **Networking** tab, choose the **LAN > IPv4 Config**
- STEP 2.** Under **DHCP**, change **DHCP Mode** to **DHCP Relay**.
- STEP 3.** Enter the IP address of the Relay gateway in **Relay Gateway**
Notice that this will block the write access to other fields, thereby disabling the DHCP server configurations
- STEP 4.** For demo purposes, we want to ensure connectivity between the SA500 and your PC, so do not apply these changes:
- STEP 5.** Click **Reset** to disregard this configuration.

IPv6 Settings

IPv6 is the next-generation Internet networking protocol and is intended to supersede the currently-used IPv4 protocol, which is limited in address space and flexibility it provides.

Internet Service Providers, PC manufacturers, and government agencies worldwide are adopting IPv6 so this standard will be the de-facto standard in the upcoming years.

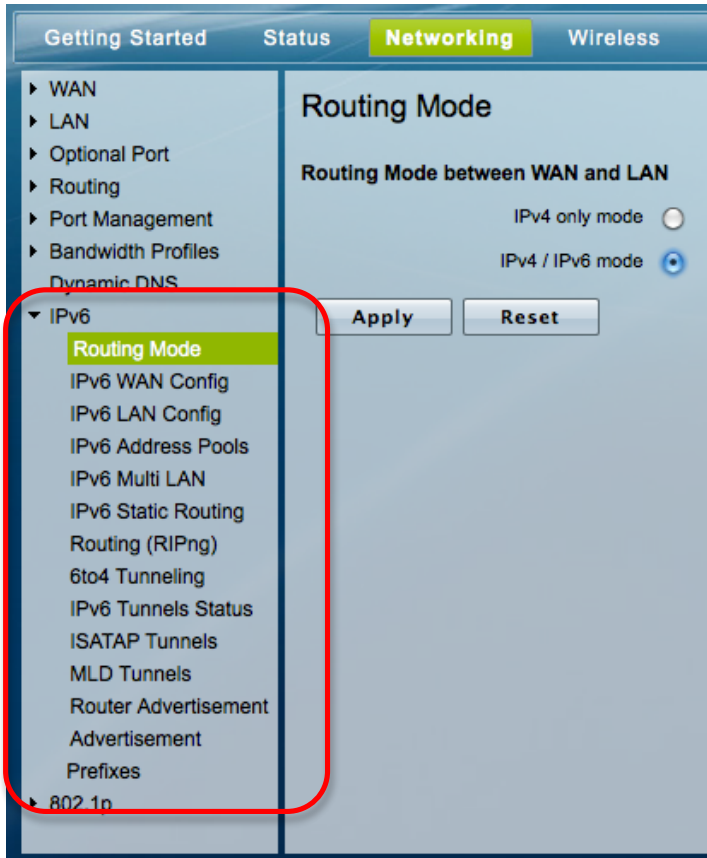
The SA500 Security Appliances already provide IPv6 capabilities, to provide scalability into future network configurations, therefore providing future protection, and decreases cost of ownership.



Note The 300 Series provides a Dual-stack mechanism, meaning it can translate between IPv4 and IPv6, depending on the network, and thereby allowing a healthy migration between the 2 standards.

The menu to configure IPv6 settings is available on the **Networking** tab, under **IPv6**.

More information on IPv6 configuration can be found in the SA500 Administration Guide.

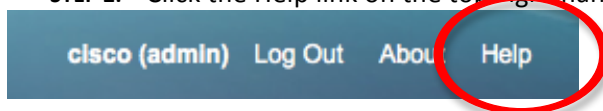


Using the On-Box Help

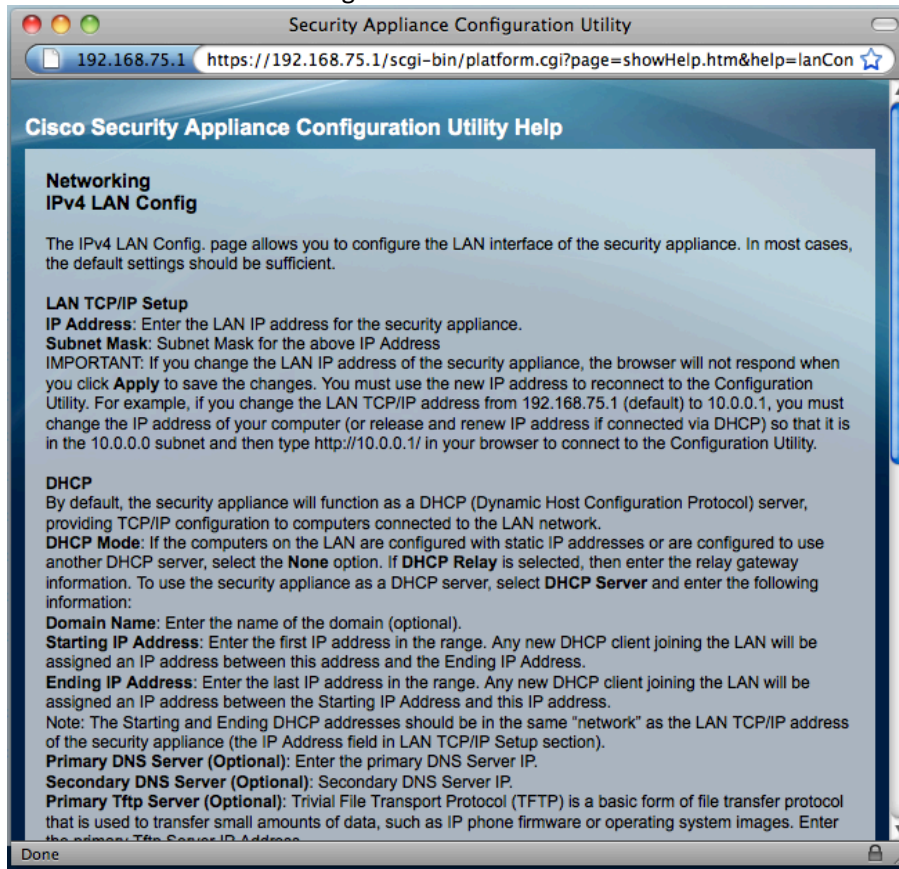
A context-sensitive Help menu is available, to help network administrators with configuration information and general knowledge about the configuration options. This comes in handy when questions arise on on-site networking configuration options and possibilities.

During this demonstration it is important to showcase and underscore the ease-of-use, intuitive and helpful management interface, and leadership compared to similar products.

- STEP 1.** From the **Getting Started/Basic page**, go into **LAN Settings**. Alternatively you can reach this link by going into the **Networking** tab, then **LAN > IPv4 Config**
- STEP 2.** Click the Help link on the top-right hand side of the Web configuration page.



- STEP 3.** This link will open a new window with information about the page you are currently viewing – IPv4 LAN Config



Note More Help information is available at <http://www.cisco.com/go/sa500help/>


Viewing System Information

Following your setup, it is convenient to see your settings in a consolidated manner, and also to test if your settings were done accurately.

Much information can be found under the **Status** menu – such as network information and connectivity status, wireless configuration and statistics, VPN connections and its users, Hosts that reside on the LAN interface and are known to the device – all of which provide vast means of verifying the device’s installation, and debugging it, if needed.

In addition, the SA500 management interface provides logs that show the history of events, some of help to explain problems in configuration, and gives the user or installer means to debug the installation, if needed.

Walk through the many options of Status information provided in the menu, and how these pages come in handy for different scenarios. They are shown below highlighted in red



The screenshot displays the SA500 management interface. The top navigation bar includes tabs for Getting Started, Status (highlighted in green), Networking, Wireless, Firewall, and IPS. A red box highlights the left-hand navigation menu, which contains the following items:

- ▼ Device Status
 - Device Status (highlighted in green)
 - Resource Utilization
 - Interface Statistics
 - Port Statistics
 - Wireless Statistics
- ▼ VPN Status
 - IPSec Status
 - SSL VPN Status
 - QuickVPN Status
- Active Users
- ▼ View Logs
 - View All Logs
 - IPSec VPN Logs
 - ProtectLink Logs
- CDP Neighbor
- LAN Devices

The main content area is titled "Device Status" and is divided into three sections:

- System Info**
 - System Name: Cisco
 - Primary Firmware Version: 1.1.19
 - Secondary Firmware Version: 1.1.19
 - Latest Image Available: [Configure Automatic Updates](#)
 - Link to Release notes:
 - Time at which last query was made:
- ProtectLink License Info**
 -  Cisco ProtectLink service has not been activated.
- LAN Info**
 - MAC Address: 00:22:6B:18:C1:04
 - IPv4 Address: 97.0.0.2 / 255.0.0.0

Advanced Demo

This set of demonstrations centers on more advanced security features that the SA500 Routers have to offer.

Throughout your demonstration, highlight and showcase the intuitive management interface, and how simple and quick it is to secure a Small Business network. While easy-to-use, the SA500 platform is a tested and qualified working system that protects your network from malware, attacks and strangers attempting to access sensitive business information.

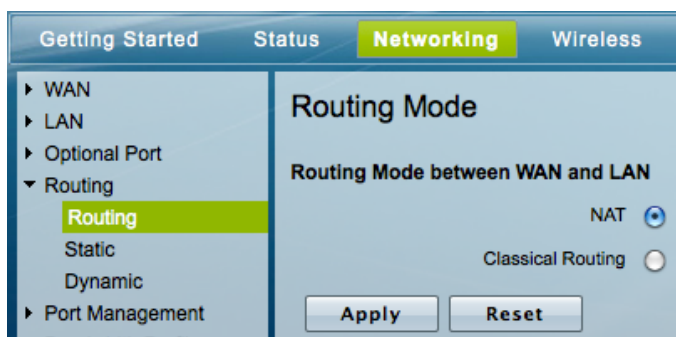
Moreover, the SA500 easily provides mobility to small businesses, by easily creating VPN tunnels between remote workers or offices in different geographic locations. This increases productivity by allowing employees to work remotely – from home or on the road, or expand to different geographic locations without jeopardizing security.

This section will cover the following scenarios:

- Creating a VPN Tunnel for Remote Worker
- Creating a VPN Tunnel from a branch office to a Main office
- Content Filtering
- Firewall rules
- Demilitarized Zone (DMZ)

This Demonstration is easier to perform when the SA500 is operating in regular Routing mode, whereas the default value is to route via NAT (Network Address Translation). Ensure that your settings reflect this configuration.

To do this, go to **Networking** menu, then navigate to **Routing > Routing** page. Click the **Classical Routing** checkbox, and click **Apply**.

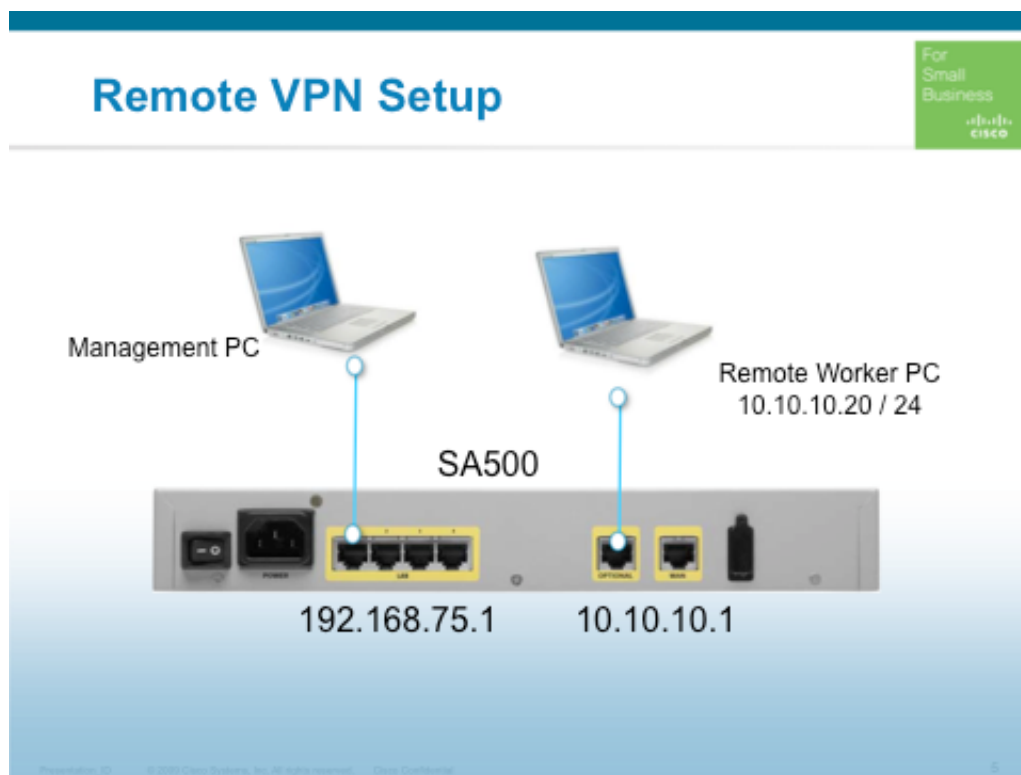


Mobility

IP Security (IPSec) VPN capabilities built into platforms like the SA500 and the RV120W enable remote Small Business employees and partners, whether working from home or on the road, to connect to your office network, access files and transfer data as securely as if they were in the office. This demonstration shows how simple creating a new VPN client account can be.

This demonstration is not meant to show a live VPN connection over the Internet. To show capability, plug in your alternate PC, simulating the Remote Worker into the Optional WAN port of the SA500. Ensure that the optional port is enabled. Configuration instructions will appear below.

The setup should look like this:



IPSec Virtual Private Network (VPN) Client Account Setup

This set of actions demonstrates how easy it is to allow access to a remote worker, whether on the road or using his broadband connection from home.

- STEP 1.** Connect a PC to the Optional WAN port of the SA500. This PC will be referred to as "Remote Worker PC". Leave your management PC on the LAN side of the SA500.
- STEP 2.** From your management PC, login to the SA500 by opening a web browser. Enter "cisco" as both username and password.
- STEP 3.** Go to **Networking > Optional Port > Optional Port mode** and set the Optional WAN interface to **WAN**. Click Apply to save our settings.

- STEP 4.** Set the Optional WAN interface to 10.10.10.10 (from **Networking > Optional Port > WAN**)
Set the Remote Worker PC's IP address to 10.10.10.20
From the Remote Worker PC, ping the management PC, or the Smart Storage device on the LAN side of SA500. Notice that connection is forbidden and that ICMP ping messages cannot go through.



Note Step 3 demonstrates a typical case of malicious attacks that can (and do) happen on a regular basis in a Small Business environment, and how the SA500 protects against it.

Attacks can range from coordinated SPAM attacks, or simply by a single user trying to enter a private network to obtain sensitive information. The latter is demonstrated in this step. We will next show how trusted users can be allowed access to the company's network, by a few simple steps.

- STEP 5.** In the SA500, Click on the **IPSec Users** menu.
- STEP 6.** Click **Add** and type the **new client's user name** and **password**. Re-enter the **password** to confirm.
Configure **Remote Peer Type** to be **Cisco QuickVPN**. Click **Apply** to create the new VPN client account. If you'd like the VPN client to be able to change his/her password, click **yes** in the Allow user to change their password radio button.
- STEP 7.** Go to **Network Management** tab, then navigate to **Remote Management**.
Enable remote Management by checking the **Enable Remote Management?** checkbox
- STEP 8.** From the Remote Worker PC, operate the QuickVPN IPSec VPN client. Enter the user's credentials, as you have configured them in Step 6.
- STEP 9.** From the Remote Worker PC, ping the management PC, or the Smart Storage device on the LAN side of SA500. Notice that connection is now allowed and that ICMP ping messages pass through freely.



Note To demonstrate a live VPN connection, the SA500 router must have WAN connectivity and the remote client connecting to the VPN router must reside on the Internet. The remote PC must have IP Sec VPN client software such as the QuickVPN client software installed and configured in order to connect.

Key Messages

- Remote Access VPN provides a secure connection across the public Internet between an employee's small business network and their laptop when working from home or out on the road.
- Enhances productivity while staying connected to the small business network to transfer files and use applications.

OPTIONAL: SSL VPN & Client Portal Setup

Secure Sockets Layer (SSL) VPN capabilities are built into the SA500 to enable remote workers to connect to your office network with a standard Web Browser (that is, no IPSec VPN client) to access files and transfer data as securely as if they were in the office. This demonstration shows how simple creating a new SSL VPN portal and client account can be. Moreover, this demonstration shows how easy it is to differentiate the access appearance of various groups with their access to the network. This demonstration shows a live VPN connection over the Internet.

- STEP 1.** Connect a PC to the Optional WAN port of the SA500. This PC will be referred to as "Remote Worker PC". Leave your management PC on the SA500's LAN side.
- STEP 2.** Login to the SA500 by opening a web browser. Enter "cisco" as both username and password.
- STEP 3.** Click the **VPN** tab.
- STEP 4.** Click the **SSL VPN Server** function, then **Portal Layouts**.
- STEP 5.** Click **Add** and enter **SSL Portal Layout** for device. This will create the portal that the remote user will access. Under **SSL VPN Portal Pages to Display**, click on the **VPN Tunnel page**.
Click **Apply**
This will lead you to the Portal Layouts page, where the Portal URL will be set. The remote user will use this URL to create a VPN tunnel later on in the demonstration.
- STEP 6.** We'll now proceed to create an SSL user, with which the Remote PC will log into the network.
Go to **Administration** tab, and then click **Users > Users**
- STEP 7.** Click **Add**, and enter the Remote user's information. Notice the following:
User Type: SSL VPN User
Select Group: SSLVPN
- STEP 8.** Select **SSL VPN Client**.
- STEP 9.** For **Client IP Address Range, Client Address Range Begin**, enter: 192.168.251.1. For **Client Address Range End**, enter 192.168.251.254. For **LCP Timeout** enter 60 seconds.
- STEP 10.** From the Remote Worker's PC, access the portal you've created in Step 5.
- STEP 11.** Select **VPN Tunnel**. Click on **SSL VPN Tunnel Client Installer/Launcher** (image shown below).



- STEP 12.** An SSL VPN client is then launched through the Browser. A virtual "network adapter" with an IP address, DNS and WINS settings is automatically created, which allows local applications to talk to services on the private network without any special network configuration on the remote SSL VPNClient machine.
- STEP 13.** To close the SSL VPN connection, logout and then close the browser.



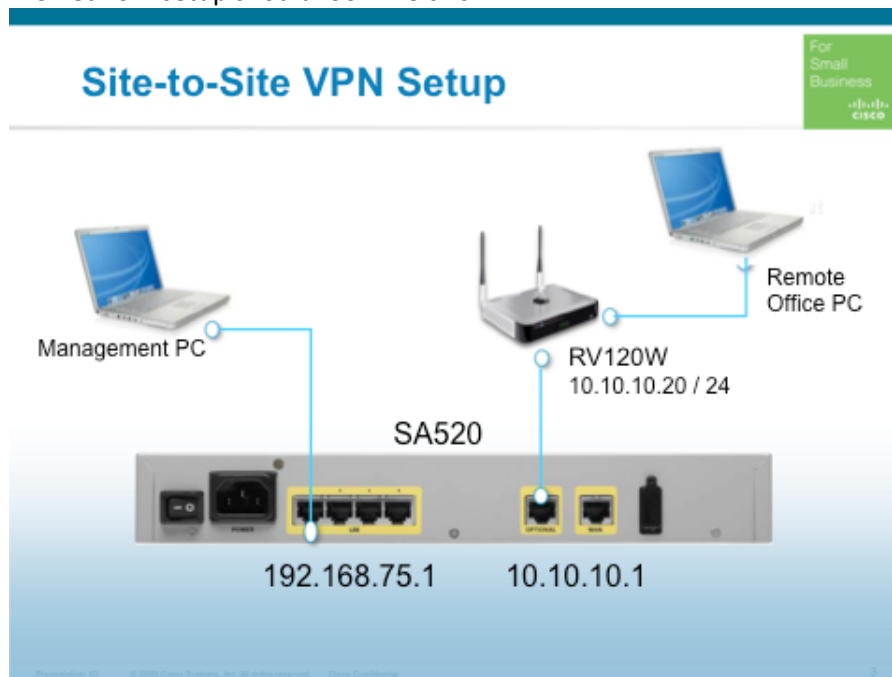
Note To demonstrate a live VPN connection, the SA500 (or RV120W) router must have WAN connectivity and the remote client connecting to the VPN portal must reside on the Internet.

Site-to-Site Virtual Private Network (VPN) Setup for Remote Office Locations

Small Businesses that expand their business geographically will typically open locations in areas remote to the main office. This set of actions demonstrates how easy it is to “combine” the two sites into one virtual office, as if they were in the same physical location.

During this demonstration, highlight the ease-of-use in quickly connecting two remote sites into a single virtual network. Showcase the uniform management interface that runs along Cisco’s various tiers of networking products.

The network setup should look like this:



- STEP 1.** As shown in the Getting Started Guide - Connect the RV120W to the Optional WAN port of the SA500. The RV120W is the gateway to the remote office’s site.
- STEP 2.** Connect a laptop to the RV120W’s LAN and let it get an IP address from the RV120W’s DHCP Server.
- STEP 3.** From your management PC, login to the SA500 by opening a web browser. Enter “cisco” as both username and password.
- STEP 4.** Go to **Networking > Optional Port > Optional Port** mode and set the Optional WAN interface to **WAN**. Click **Apply** to save our settings.
- STEP 5.** Leave the Optional WAN interface as 10.10.10.1

Set the RV120W's WAN IP address to 10.10.10.20

From the laptop connected to RV120W, ping your management PC, or the Smart Storage device on the LAN side of SA500. Notice that connection is forbidden and that ICMP ping messages cannot go through.



Note Step 3 demonstrates very well a typical case of malicious attacks that can (and do) happen on a day-to-day basis in a Small Business environment, and how the SA500 protects against it.

Attacks can range from coordinated SPAM attacks, or simply by a single user trying to enter a private network to obtain sensitive information. The latter is demonstrated in this step. We will next show how trusted users can be allowed access to the company's network, by a few simple steps.

- STEP 6.** Click the **VPN** tab.
Click the **VPN Wizard** tab and talk through how the Wizard easily helps you to set up a VPN Server for the small business.
The fields on this page should be completed as follows:
Select VPN Type: Site-to-Site
Connection Name: assign a name that will be easily remembered
Local WAN Interface: Dedicated WAN (per setup of this demo. See Step 1)
Remote / Local WAN Addresses: IP Address
Remote WAN's IP Address: 10.10.10.20
Local WAN's IP address: 10.10.10.10
Remote LAN IP Address: 192.168.1.0 (this is the RV120W's LAN IP subnet)
Remote LAN Subnet Mask: 255.255.255.0
- STEP 7.** Click Apply when finished. This will lead you to VPN Policies menu, in where you will see the policy you have just created. Click on the **Edit** button on the right side of that row.
- STEP 8.** Disable **NetBios** by un-checking the checkbox
Set **Remote Traffic Selection** to **Any**
- STEP 9.** Logon to the RV120W using the PC on that LAN.
- STEP 10.** Go to VPN menu and click **IPSec > VPN Wizard**. This is the same page as you have just configured in the SA500. Show how Cisco has kept the same look and feel on all its products, including similar pages
- STEP 11.** The fields on this page should be completed similarly to that of SA500, as follows:
Connect to...: Gateway
Connection Name: use the connection name entered in Step 5
Remote / Local Gateway Type: IP Address
Remote WAN's IP Address: 10.10.10.10
Local WAN's IP address: 10.10.10.20
Remote LAN IP Address: 192.168.75.0 (this is the SA500's LAN IP subnet)

Remote LAN Subnet Mask: 255.255.255.0

Click **Apply**

- STEP 12.** You will be redirected to **IPSec Policies** page, where you will see the entry you've created.
- STEP 13.** Click on the link **IPSec VPN Connection Status** on that page to connect to SA500
- STEP 14.** After creation of the IPSec VPN tunnel you will be directed to **Status > IPSec Connection Status**, where the connection status will be shown in the **State** column.
An active connection will be listed as [IPsec SA Established](#)
- STEP 15.** You can also test this from the SA500 management interface, by going to **Status** tab, then to **VPN Status > IPSec Status**. The connection entry will appear with a state of **IPSec SA Established**
- STEP 16.** From the laptop connected to RV120W, ping the management PC, or the Smart Storage device on the LAN side of SA500. Notice that connection is now allowed and that ICMP ping messages pass through freely.



Note To demonstrate a live VPN connection, the SA500 router must have WAN connectivity and the RV120W must reside on the Internet

Key Messages

- Site-to-Site VPN provides a secure connection across the public Internet between two geographically remote sites of a small business, thereby allowing them to be virtually in the same office environment.
- Allows small businesses to easily expand geographically, without jeopardising security
- Enhances productivity while staying connected to remote peers, by sharing access to local material and applications usage.
- Uniform management interface among different tiers of Cisco's Small Business product line, which makes it easier to configure and manage, with or without a dedicated IT staff.

Firewall

Protecting your network from malicious attacks is something that is the utmost importance to the business owner. Unauthorized users or applications always attempt to access sensitive information on the internal network or to implant viruses. It is there essential to understand how SA500 will provide this level of security, with a simple configuration that provides future peace of mind.



Note Leave the network setup as in the IPSec VPN setup. Disconnect the VPN connection you have created, as we will want to simulate unsecure/untrusted traffic

- STEP 1.** Login to the SA500 by opening a web browser. Enter “admin” as both username and password.
- STEP 2.** Go to **Firewall** tab, then navigate to **Firewall > IPv4 Rules**. You can also access this page by clicking Login to the SA500 by opening a web browser. Configure Firewall and NAT Rules, from the Getting Started (Advanced) page.
This page will show the available firewall rules.
- STEP 3.** Check that the Remote PC, connected to the Optional WAN is unable to ping the management PC on the LAN side.



Note All traffic incoming from the WAN will be blocked by default. However all devices on the company network (LAN side) will have access to the Internet.

To change this setting, go to **Firewall** on the menu bar, then click **Firewall > Default Outbound Policy** in the navigation tree.

Select **Allow Always** to allow outbound traffic, or choose **Block Always** to block outbound traffic.

Click **Apply** to save your settings, or click **Reset** to revert to the saved settings.

- STEP 4.** We will now add a firewall rule to enable ICMP packets to flow through to the LAN, and deem them safe
- STEP 5.** Click **Add** to create the firewall rule. Populate the fields with the values below:
Show how versatile the SA500 is by allowing many configurations for traffic enablement – the many permutations configuring trusted source, service (protocol), destination etc. allow the business owner flexibility in managing the network’s security.
 - From Zone:** INSECURE (Dedicated WAN/Optional WAN)
 - To Zone:** SECURE (LAN)
 - Service:** PING ← Select from the drop down menu. Here you can play around with other protocols
 - Action:** ALLOW always
 - Source Hosts:** Single Address ← you can also configure to **Any**
 - From:** 10.10.10.20

Destination NAT Setting – Internal IP Address: 192.168.75.x ← your management PC
Click **Apply**

- STEP 6.** Try to ping from the Remote PC to the LAN PC and verify that ICMP ping messages are passing through.
- STEP 7.** As a follow on, you can demonstrate other protocols or block-settings by creating additional firewall rules and testing them via other communication applications (such as FTP, TFTP, HTTP, and so on).

Content Filtering

Protecting a network's privacy as well as network security come hand-in-hand with Content Filtering. In this demonstration section, we show the many advantages of web and content filtering, not only as a method to secure a network, but also as a means to raise productivity with a Small Business.

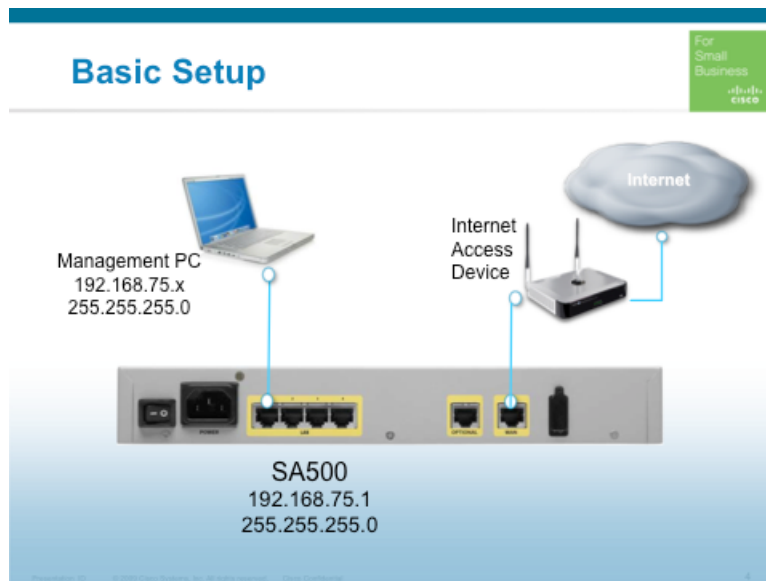
Filter URLs

Productivity is an essential part of a small business day-to-day life. When productivity decreases due to employee's web surfing, social networking or use of personal email accounts, employees become less productive, which hurts the bottom line. The SA500 can quickly limit the access to certain web sites that reduce productivity as demonstrated here.

In addition, filtering URLs that are inappropriate, don't match the company's values or waste valuable bandwidth is recommended, and is simple to set up.

In this demonstration, we demonstrate how access from the LAN side (simulating a user in the day-to-day environment) to the popular social networking site facebook can be denied from the office network.

This demonstration uses the Basic setup as see below:



- STEP 1.** From your management PC, open a web browser and connect to facebook.com. Ensure that you can access this site and navigate through it.
- STEP 2.** Login to the SA500 by opening a web browser. Enter "cisco" as both username and password
- STEP 3.** Go to **Firewall** tab, and then navigate to **Content Filtering > Content Filtering**. Enable Content Filtering by checking the **Enable Content Filtering** radio button and clicking **Apply**
Show that you can configure various web components (ActiveX, Java, Proxy, Cookies) to be blocked from entering the network, by checking the appropriate boxes.
Leave these unchecked for this demo.
- STEP 4.** Now, let's configure URLs that we want to prevent employee's access to (such as social networking sites, or those known to have inappropriate content, for example)

- STEP 5.** From the **Firewall** tab and **Content Filtering** menu, which you are already on, go to **Blocked URLs** page. The Blocked URLs will appear in this page.
- STEP 6.** Click **Add**. Enter the following information in the configuration page:
URL: facebook ← you can enter multiple entries, by separating them with semicolons(;) **Match Type:** URL Keyword
Click **Apply** and return to the Blocked URLs page.
- STEP 7.** Repeat step 1. See how you are now unable to reach this web site, now that it is blocked by the SA500.

DMZ Setup

If your business hosts public services such as web sites, you need a way to allow access to those services without exposing your LAN. If your web server is hosted in your premise, you can potentially expose your internal network to malicious users that access your web server. By placing your public services on a DMZ (Demarcation Zone or Demilitarized Zone), you can add an additional layer of security to your local network. This zone acts as a separate network between your private LAN and the Internet. The public can connect to the services on the DMZ but cannot penetrate the LAN. You should configure your DMZ to include any hosts that must be exposed to the WAN (such as web or email servers). After you configure your DMZ, you can configure the firewall rules that enable traffic to connect only to the services that you specify.

In this demonstration, we attach a device that simulates a web server to the Optional WAN, and configure that port to act as the DMZ. We then configure the firewall settings so that external users will get access only to the DMZ, but not to the LAN, so the latter will stay protected.

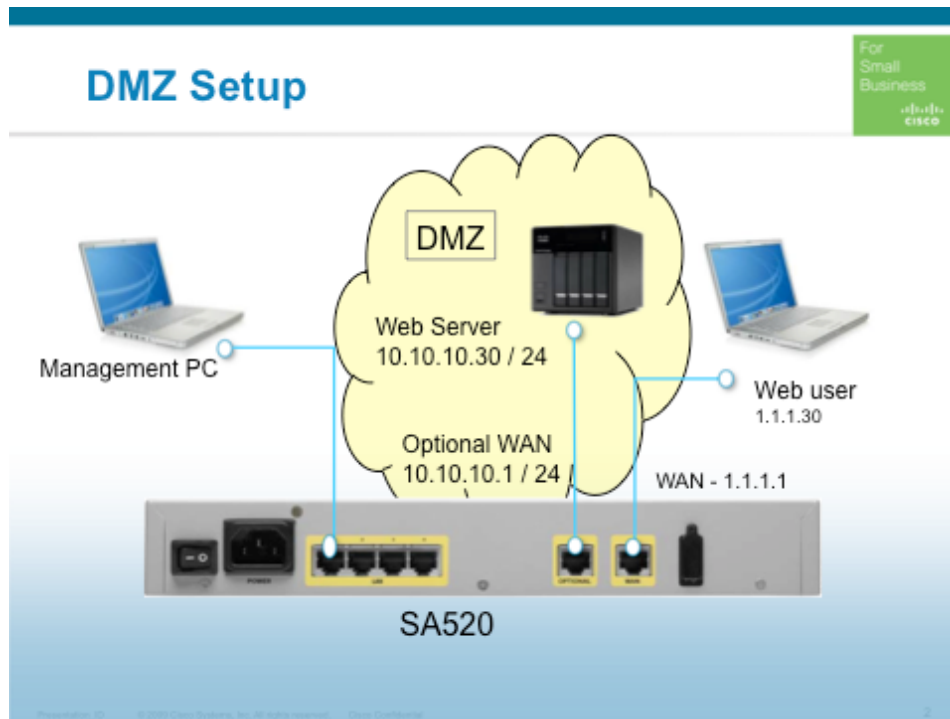
For this demo you need 3 PCs: (1) management PC that will configure the SA500 from the LAN side; (2) a PC to simulate an external user, which will be connected to the WAN port; (3) Another device (either PC or an NSS32x) will act as the web server on the DMZ, and will be connected to the Optional WAN port.

If you don't have 3 PCs, you can use your management PC as a web user (connected to WAN port) and alternate between those two functions. In this case, please make sure you are well aware of the network settings, and are very familiar with how to change the IP address on your PC.

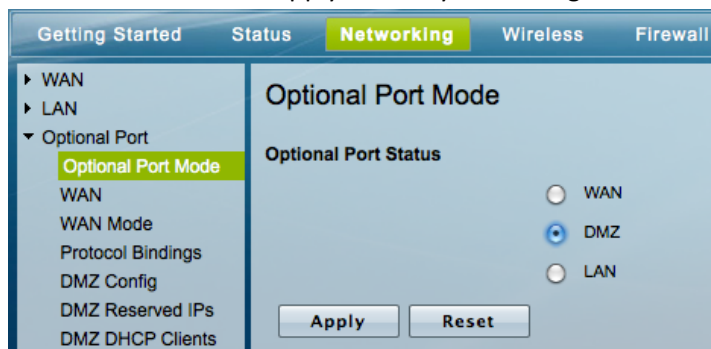
Key Messages

- Protect the Small Business network by allowing incoming traffic only to secure areas (DMZ)
- Show how the process of securing your network by configuring a DMZ, is straightforward and easy.
- Show how the step-by-step process is embedded in the **Getting Started (Advanced)** page, under **DMZ**. Following the links from top to bottom in this section will naturally direct you to the correct settings.

The setup should look like this:



- STEP 1. From your management PC, Login to the SA500 by opening a web browser. Enter “cisco” as both username and password.
- STEP 2. Go to **Networking** tab, then navigate to **Optional Port > Optional Port Mode**. You can reach this page through the Getting Started (Advanced) page as well – under DMZ port, click **Set Optional Port to DMZ Mode**.
- STEP 3. Choose **DMZ** and click Apply to save your settings.



- STEP 4. Click **Networking** on the menu bar, then click **Optional Port > DMZ Config** in the navigation tree. You can reach this page also from the Getting Started (Advanced) page, by clicking **Configure DMZ Settings**
- STEP 5. In the DMZ Port setup page, enter an IP Address and the subnet mask for the DMZ port on the internal network. Set values as follows:
IP Address: 10.10.10.1

Subnet Mask: 255.255.255.0

DHCP Mode: None ← this option assumes that IP addresses are manually set on web server
Show how versatile the SA500 is, that it provides the option to dynamically assign IP addresses to servers on the DMZ. This makes it easier for system administrators, especially with CCA that can find devices on the network.

STEP 6. Configure your device connected to the Optional WAN port (simulating the web server), to IP address 10.10.10.30.

Verify that you can ping the Optional WAN port – 10.10.10.1

STEP 7. Now, we will configure the WAN port so that the demo can be shown.

Go to **Networking** on the menu bar, then click **WAN > IPv4 Config**. Under **Internet (IP) Address**, select **Use Static IP Address** for **IP Address source** field.

IP Address: 1.1.1.1

IP Subnet Mask: 255.255.255.0

The following 2 fields are required to have values, but are not required for this demo:

Gateway IP address: 1.1.1.1

Primary DNS Server: 192.168.75.1

STEP 8. On the Web User PC, change the IP address to 1.1.1.30 and try to ping the SA500 WAN interface – 1.1.1.1. Packets will not go through, as firewall rules are not applied. We will show this in the next steps of this demonstration.

You can test connectivity by going into the **Administration > Diagnostics** page and running a ping test to 1.1.1.30. See that packets are following through.

STEP 9. From the Web user PC, try to ping the “web server” 10.10.10.30 and see that packets do not go through.

STEP 10. We’ll now proceed to configure a firewall rule that will allow inbound traffic from the WAN side (Web user) to access your servers on the DMZ. Show how you can specify a public IP address for a server on your DMZ, if applicable.

Go to **Firewall** on the menu bar

STEP 11. To get started, click **Firewall** on the menu bar. Go to **Firewall > IPv4 Rules**. The Firewall rules page appears with all available firewall entries. Show how you can easily filter through the entries using the **Select Rules** options. This comes in handy when many rules are configured.

STEP 12. Click **Add** and a new entry form will appear. This is the same step you have followed in the Firewall demonstration.

STEP 13. Enter the following values into the new firewall rule:

From Zone: UNSECURED (Dedicated WAN/Optional WAN)

To Zone: DMZ

Service: PING



Note We use the PING option for this demonstration since a web server is not easily accessible for demo purposes, however in real life scenarios, you would want to configure this to be HTTP or HTTPS

Action: ALLOW Always

Internal IP Address: 10.10.10.30

Click **Apply** to save this rule

STEP 14. Click **Add** once more to allow the flow of traffic from the DMZ to the WAN network. Enter the following values:

From Zone: DMZ

To Zone: UNSECURED (Dedicated WAN/Optional WAN)

Service: PING

Action: ALLOW Always

Internal IP Address: 10.10.10.30

Click **Apply** to save this rule

STEP 15. Now that the firewall settings are applied, from the Web user PC, try to ping the “web server” 10.10.10.30 and see that packets are following through.

Try to ping the LAN side PC (Management PC) or the LAN gateway and verify that packets are denied access

Unified Threat Management

Intrusion Prevention System

- STEP 1.** Login to the SA500 by opening a web browser and going to
- STEP 2.** Enter “**cisco**” as both the username and password.
- STEP 3.** Click the **IPS** tab.
- STEP 4.** Next to IPS Function, click the **Enable IPS Protection for LAN** radio button, and then click **Apply**. Below in the Automatic Signature Update area, enter your Cisco.com username and password for automatic signature updates and click **Apply**. Alternatively, select **Browse** and locate the new updated signature file downloaded from Cisco.com, then click **Upload**.
- STEP 5.** Next to **IPS Policy**. The LAN and DMZ are 2 different networks and you can set up different policies for them to address different traffic patterns on trusted vs. untrusted networks. Click the IPS policies tab. Detect only is intrusion detection. Detect and Prevent will detect and block (prevention).
- STEP 6.** Next to **Protocol Inspection**. Choose from list of common protocols to inspect like FTP.
 - **Disabled**: Select this option to disable check for this category.
 - **Detect Only**: Select this option to enable check for this category and log a message upon detection.
 - **Detect and Prevent**: Select this option to enable check for this category. Upon detection, a message is logged, and appropriate action is taken to prevent the attack.
- STEP 7.** Next to **IM and P2P Blocking**. Click the IM and P2P Blocking Settings to allow or disable access for Peer-to-Peer and Instant Messaging services. If changes were made click **Save Settings**.
- STEP 8.** The router must have a WAN connection in order for IPS to intercept malicious packets. If not connected to a live WAN connection do so. With the demo PC connected to the router as a client browse the Internet for a while and allow adequate time for the WAN connection to have some uptime.
- STEP 9.** View the IPS logs - Click the **IPS** tab of the SA500 web interface and then to **IPS Setup**. Under IPS Status check **View IPS Logs**. Notice any activity blocked by the IPS system, for example TCP Portsweeps.
- STEP 10.** You can also view IPS logs under **Status** tab of the SA500 web interface and then to **View Logs** and then **View All Logs**. This will provide local log information of the installed IPS signature.

Web Threat Protection (Cisco ProtectLink Gateway or Cisco Protectlink Web Services)

Web threat protection is a subscription-based ‘add-on’ for SA500 - available with both the Cisco Protectlink Gateway service and the Cisco Web Protection service. Cisco ProtectLink Web helps protect businesses from malware by blocking access to known dangerous websites and provides web filtering to prevent access to inappropriate content, helping increase employee productivity.

The Web threat protection demonstration requires the SA500 router to be connected to a live Internet connection. The demonstration will first cover the initial installation of the ProtectLink Gateway or Web Service followed by a URL filtering overview. URL filtering is a great demonstration for business owners and managers looking to increase productivity by limiting Internet access to employees.

Demonstrate Steps 2 -15 if this is the first time setting up Protectlink on SA500.

- STEP 1.** Login to the SA500 by opening a web browser/Enter “cisco” as both username and password
- STEP 2.** Click the **Protect Link** tab.
- STEP 3.** Click **I have purchased ProtectLink Gateway and want to register it** link. A browser window open.
- STEP 4.** Enter your **ProtectLink Registration Key** in the fields (note, to get Cisco internal ProtectLink Registration keys, please contact enoy@cisco.com). Click **Next**.
- STEP 5.** Read and if you agree accept the License Terms, click **I Accept** and then click **Submit**.
- STEP 6.** Click **Continue Registration**.
- STEP 7.** Enter the appropriate registration information then click **Submit**.
- STEP 8.** Confirm the registration information, then click **OK**.
- STEP 9.** The activation code will appear in the browser window and will also be e-mailed to the submitted e-mail address. Write the activation code down to be used to finalize the ProtectLink installation process.
- STEP 10.** Go back to the ProtectLink tab within the SA500 web interface.
- STEP 11.** Click **I have my Activation Code (AC) and want to activate ProtectLink Gateway**.
- STEP 12.** Enter the activation code in the appropriate fields. Click **Next** when finished.
- STEP 13.** Click **Next** again if the displayed license information is correct.
- STEP 14.** **Refresh** the ProtectLink page until the Trend Micro Web Protection page appears. Depending on the speed of the SA500’s Internet connection, it may take a few minutes for the Trend Micro Web Protection interface to appear in the routers web interface. Another e-mail will be sent by Trend Micro after the gateway has been successfully activated.

Demonstrate Steps 15 onwards if you have already registered Cisco Protectlink Gateway and the service is connected to WAN and active.

- STEP 15.** Open a new browser tab or window and go to **Protectlink** tab. Next to **Web Protection** function, click **Web Threat Protection**, then click the **Enable Web Threat Protection** button. Choose a security level (default is Medium) and then click **Apply**.
- STEP 16.** Next to **URL Filtering**. Click the **Enable URL Filtering** button. Define the Business **day** and **time** for the URL filtering rules to be active. For this demonstration All Day will be used for the time. When choosing to use specific business hours, time outside of this range will be considered leisure time.

- STEP 17.** Review the **Filtered Categories**. Expand the General URL filter category by clicking the **plus** icon in URL Categories (that is, Social).
- STEP 18.** Click the **checkbox** next to Social Networking under the Business Hours column (or other bandwidth hungry services like Adult, Gambling). If wanting to block URLs during leisure time be sure to place an additional check mark next to leisure time.
- STEP 19.** Click **Apply** to save any changes.
- STEP 20.** Using a web browser, browse to Facebook and notice the URL has been blocked. A message will appear notifying access has been blocked.
- STEP 21.** Go back to the **ProtectLink** tab in the SA500 web interface to show the **Web Protection** then **URL Filtering** page. Refresh this page and notice the number of **Instances Blocked** within the General category, which shows the number of times a filtered URL category has been invoked.
- STEP 22.** Enable other various URL filtering categories based on the customer's specific small business needs.
- STEP 23.** Define any Approved URLs needed by your customer to show how approved websites can be access if blocked by filtering rules.
- STEP 24.** Define any Approved clients as needed by your customer to show how specific clients can be excluded from URL filtering.

OPTIONAL: Email Protection (Cisco ProtectLink Gateway Service only)

Email protection is another 'add-on' for the SA500 available with the subscription-based Cisco ProtectLink Gateway Service only. The email Protection demonstration utilizes Trend Micro™ InterScan Messaging Hosted Security to delivers high-performance, cost-effective hosted security services that protect businesses from spam, viruses, and inappropriate content before they reach the network through email messages. Email filtering is a great demonstration for business owners and managers looking to increase productivity by reducing email SPAM and viruses and malware carried through email.

- STEP 1.** Login to the SA500 by opening a web browser. Enter "cisco" as both username and password
- STEP 2.** Click the **Email Protection** tab. Select US or Europe Protectlink Email portal.
- STEP 3.** ***No need to go beyond this page unless you have Trend Micro Online Registration username and password on hand.***
At this point, explain that you go to this Hosted Email Security configuration page to configure a domain for email protection to work. You need your own domain (for example, www.bobsit.com) and you then point the protection domain to the Trend Micro™ InterScan Messaging Hosted Security service. So all your email gets redirected to that service, scanned and filtered, then passed on to the local email server. Essentially, ProtectLink sits between the world and your email service, and filters your email traffic as a service.
- STEP 4.** If you are asked can you use an online mail server like Google for email protection, respond as follows: You have to be able to redirect MX records for your domain (for example, www.bobsit.com) to the Trend Micro service. You can't redirect the Google

mail server. But if you set up your mail server in Google docs to domain www.bobsit.com, Google can allow you to redirect your MX records. You would then set up your local email system to point to Protectlink, and then Protectlink to point to the Google service. So Protectlink sits between the World and your business, but you can still get your email from Gmail. That's not all that practical because Gmail does its own filtering, so Protectlink may be an overkill in that scenario.

OPTIONAL: Endpoint Protection (Cisco ProtectLink Endpoint Service)

Endpoint protection is available with the Cisco ProtectLink Endpoint Service. Use the Endpoint Protection service to enable policy enforcement at the endpoint level on PCs and servers. You must install the ProtectLink Agent on all clients you want to protect. The Agent ensures that only protected clients (that have this software installed) can access the Web.

This feature is important for Small Businesses with the spike in mobile users that can plug into the Small Business network, via a wireless connection, and access internal information. What the policy enforcement does is stop someone who doesn't have endpoint protection installed from accessing the Internet.

Note: Add a computer to the Approved Clients list for unrestricted Web access. See the Approved Clients page for more information.

- STEP 1.** Login to the SA500 by opening a web browser. Enter "cisco" as both username and password
- STEP 2.** Click the **ProtectLink** tab.
- STEP 3.** Click **ProtectLink Endpoint**. Click the **Enable Policy Enforcement** button.
- STEP 4.** To provide endpoint protection:
 - 1. Access the ProtectLink endpoint console from the links shown on the ProtectLink Endpoint page. You will need TrendMicro username and password (not the same as SA500).
 - 2. Create packages and install these on all clients.
 - 3. Next, download the TMAgent from <http://www.trendmicro.com/download/product.asp?productid=94>
Install the TMAgent on all clients.
- STEP 5.** Explain that if you have an endpoint that doesn't have the agent installed, the system will redirect you to a web page that says you don't have the endpoint installed before the endpoint is allowed out to the Internet.