Connect, Install, and Configure

This topic contains the following sections:

Overview of Connect, Install, and Configure

The Secure Web Appliance provides the following modes of operation:

- Standard: The Standard mode of Secure Web Appliance operation includes on-site Web Proxy services and Layer-4 traffic monitoring, which are not available in the Cloud Web Security Connector mode.
- Cloud Web Security Connector: In Cloud Web Security Connector mode, the appliance connects to and routes traffic to a Cisco Cloud Web Security (CWS) proxy, where Web security policies are enforced.

The appliance has multiple network ports, with each assigned to manage one or more specific data types.

The appliance uses network routes, DNS, VLANs, and other settings and services to manage network connectivity and traffic interception. The System Setup Wizard lets you set up basic services and settings, while the appliance's Web interface lets you modify settings and configure additional options.

Deploying a Virtual Appliance

To deploy a virtual Secure Web Appliance, see the *Cisco Content Security Virtual Appliance Installation Guide* , available from
http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Migrating from a Physical to a Virtual Appliance

To migrate your deployment from a physical appliance to a virtual appliance, see the virtual appliance installation guide referenced in the previous topic and the Release Notes for your AsyncOS version.

Comparison of Modes of Operation

The following table presents the various menu commands available in Standard and Cloud connector Modes, thereby indicating the various features available in each mode.

Menu	Available in Standard Mode	Available in Cloud Connector Mode
Reporting	System Status Overview Users User Count Web Sites URL Categories Application Visibility Anti-Malware Secure Endpoint File Analysis Secure Endpoint Verdict Updates Client Malware Risk Web Reputation Filters Layer-4 Traffic Monitor Reports by User Location Web Tracking System Capacity System Status Scheduled Reports Archived Reports	System Status

Menu	Available in Standard Mode	Available in Cloud Connector Mode
Web Security Manager	Identification Profiles Cloud Routing Policies SaaS Policies Decryption Policies Routing Policies Access Policies Overall Bandwidth Limits Cisco Data Security Outbound Malware Scanning External Data Loss Prevention Web Traffic Tap Policies SOCKS Policies Custom URL Categories Define Time Ranges and Quotas Bypass Settings Layer-4 Traffic Monitor	Identification Profiles Cloud Routing Policies External Data Loss Prevention Custom URL Categories
Security Services	Web Proxy FTP Proxy HTTPS Proxy SOCKS Proxy PAC File Hosting Acceptable Use Controls Anti-Malware and Reputation Data Transfer Filters AnyConnect Secure Mobility End-User Notification L4 Traffic Monitor SensorBase Reporting Cisco Cloudlock Cisco Cognitive Threat Analytics	Web Proxy

Menu	Available in Standard Mode	Available in Cloud Connector Mode
Network	Interfaces Transparent Redirection Routes DNS High Availability Internal SMTP Relay Upstream Proxy External DLP Servers Web Traffic Tap Certificate Management Authentication Identity Provider for SaaS Identity Services Engine	Interfaces Transparent Redirection Routes DNS High Availability Internal SMTP Relay External DLP Servers Certificate Management Authentication Machine ID Service Cloud Connector
System Administration	Policy Trace Alerts Log Subscriptions Return Addresses SSL Configuration Users Network Access Time Zone Time Settings Configuration Summary Configuration File Feature Keys Settings Feature Keys Upgrade and Update Settings System Upgrade System Setup Wizard FIPS Mode Next Steps	Alerts Log Subscriptions SSL Configuration Users Network Access Time Zone Time Settings Configuration Summary Configuration File Feature Keys Upgrade and Update Settings System Upgrade System Setup Wizard

Menu	Available in Standard Mode	Available in Cloud Connector Mode
Cisco CWS Portal(available only in Hybrid Web Security mode)	N/A	N/A

Task Overview - Connect, Install, and Configure

Task	More Information
Connect the appliance to Internet traffic.	Connect the Appliance, on page 5
Gather and record set-up information.	Gathering Setup Information, on page 8
Run the System Setup Wizard.	System Setup Wizard, on page 9
Configure HTTPS proxy settings, Authentication Realms and Identification Profiles. This step must be completed for Hybrid Web Security mode.	Enabling the HTTPS Proxy Authentication Realms Identification Profiles and Authentication
(Optional) Connect upstream proxies.	Upstream Proxies, on page 16

Connect the Appliance

Before you begin

- To mount the appliance, cable the appliance for management, and connect the appliance to power, follow the instructions in the hardware guide for your appliance. For the location of this document for your model, see Documentation Set.
- If you plan to physically connect the appliance to a WCCP v2 router for transparent redirection, first verify that the WCCP router supports Layer 2 redirection.
- Be aware of Cisco configuration recommendations:
  - Use simplex cabling (separate cables for incoming and outgoing traffic) if possible for enhanced performance and security.

Step 1 Connect the Management interface if you have not already done so:

Ethernet Port	Notes
M1	Connect M1 to where it can: • Send and receive Management traffic. • (Optional) Send and receive web proxy data traffic. You can connect a laptop directly to M1 to administer the appliance. To connect to the management interface using a hostname (http://hostname:8080), add the appliance hostname and IP address to your DNS server database.
P1 and P2 (optional)	• Available for outbound management services traffic but not administration. • Enable **Use M1 port for management only** (Network > Interfaces page). • Set routing for the service to use the Data interface.

Step 2 (Optional) Connect the appliance to data traffic either directly or through a transparent redirection device:

Ethernet Port	Explicit Forwarding	Transparent Redirection
P1/P2	P1 only: • Enable **Use M1 port for management only**. • Connect P1 and M1 to different subnets. • Use a duplex cable to connect P1 the internal network and the internet to receive both inbound and outbound traffic. P1 and P2 • Enable P1. • Connect M1, P1, and P2 to different subnets. • Connect P2 to the internet to receive inbound internet traffic. After running the System Setup Wizard, enable P2.	Device: WCCP v2 router: • For Layer 2 redirection, physically connect router to P1/P2. • For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation. • Create a WCCP Service on the appliance. Device: Layer-4 Switch: • For Layer 2 redirection, physically connect switch to P1/P2. • For Layer 3 redirection, be aware of possible performance issues with Generic Routing Encapsulation. **Note** The appliance does not support inline mode.
M1 (optional)	If **Use M1 port for management only** is disabled, M1 is the default port for data traffic.	N/A

Step 3 (Optional) To monitor Layer-4 traffic, connect the Appliance to a TAP, switch, or hub after the proxy ports and before any device that performs network address translation (NAT) on client IP addresses:

Ethernet Port	Notes
T1/T2	To allow Layer-4 Traffic Monitor blocking, put Layer 4 Traffic Monitor on the same network as the Secure Web Appliance. **Recommended configuration:** **Device: Network TAP:** • **Connect T1 to network TAP to receive outbound client traffic.** • **Connect T2 to network TAP to receive inbound internet traffic.** Other options: Device: Network TAP: • Use duplex cable on T1 to receive inbound and outbound traffic. Device: Spanned or mirrored port on a switch • Connect T1 to receive outbound client traffic and connect T2 to receive inbound internet traffic. • (Less preferred) Connect T1 using a half or full duplex cable to receive both inbound and outbound traffic. Device: Hub: • (Least preferred) Connect T1 using a duplex cable to receive both inbound and outbound traffic. The appliance listens to traffic on all TCP ports on these interfaces.

Step 4 Connect external proxies upstream of the appliance to allow the external proxies to receive data from the appliance.

What to do next

Gathering Setup Information, on page 8

Related Topics

- Enabling or Changing Network Interfaces, on page 18
- Using the P2 Data Interface for Web Proxy Data , on page 32
- Adding and Editing a WCCP Service, on page 38
- Configuring Transparent Redirection, on page 36
- Upstream Proxies, on page 16

Gathering Setup Information

You can use the worksheet below to record the configuration values you will need while running the System Setup Wizard. For additional information about each property, see System Setup Wizard Reference Information, on page 10.

System Setup Wizard Worksheet			
Property	**Value**	**Property**	**Value**
Appliance Details		**Routes**	
Default SystemHostname		**Management Traffic**	
Local DNS Server(s) **(Required if not using Internet Root Servers)**		Default Gateway	
DNS Server 1		(Optional) Static Route Table Name	
(Optional) DNS Server 2		(Optional) Static Route Table Destination Network	
(Optional) DNS Server 3		(Optional) Standard Service Router Addresses	
(Optional) Time Settings		**(Optional) Data Traffic**	
Network Time Protocol Server		Default Gateway	
(Optional) External Proxy Details		Static Route Table Name	
Proxy Group Name		Static Route Table Destination Network	
Proxy Server Address		**(Optional) WCCP Settings**	
Proxy Port Number		WCCP Router Address	
Interface Details		WCCP Router Passphrase	
Management (M1) Port		**Administrative Settings**	
IPv4 Address (required) IPv6 Address (optional)		Administrator Passphrase	
Network Mask		Email System Alerts To	

System Setup Wizard Worksheet			
Property	**Value**	**Property**	**Value**
Hostname		(Optional) SMTP Relay Host	
(Optional) Data (P1) Port			
IPv4 (optional) IPv6 Address (optional)			
Network Mask			
Hostname			

System Setup Wizard

Before you begin

- Connect the Appliance to networks and devices. See Connect the Appliance, on page 5.
- Complete the System Setup Wizard worksheet. See Gathering Setup Information, on page 8.
- If you are setting up a virtual appliance:
  - Use the `loadlicense` command to load the virtual appliance license. For complete information, see the *Cisco Content Security Virtual Appliance Installation Guide*, available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.
  - Enable the HTTP and/or HTTPS interfaces: In the command-line interface (CLI), run the `interfaceconfig` command.
- Note that reference information for each configuration item used in the System Setup Wizard is available at System Setup Wizard Reference Information, on page 10.

Warning Only use the System Setup Wizard the first time you install the appliance, or if you want to completely overwrite the existing configuration.

Step 1 Open a browser and enter the IP address of the Secure Web Appliance. The first time you run the System Setup Wizard, use the default IP address:

`https://192.168.42.42:8443`

-or-

`http://192.168.42.42:8080`

where `192.168.42.42` is the default IP address, and `8080` is the default admin port setting for HTTP, and `8443` is default admin port for HTTPS.

Otherwise, if the appliance is currently configured, use the IP address of the M1 port.

Step 2 When the appliance login screen appears, enter the user name and passphrase to access the appliance. By default, the appliance ships with the following user name and passphrase:

- User name: `admin`
- Passphrase: `ironport`

Step 3 You must immediately change the passphrase.

Step 4 Choose **System Administration > System Setup Wizard**.

If the appliance is already configured, you will be warned that you are about to reset the configuration. To continue with the System Setup Wizard, check **Reset Network Settings**, and then click the **Reset Configuration** button. The appliance will reset and the browser will refresh to the appliance home screen.

Step 5 Read and accept the terms of the end-user license agreement.

Step 6 Click **Begin Setup** to continue.

Step 7 Configure all settings using the reference tables provided in the following sections as required. See System Setup Wizard Reference Information, on page 10.

Step 8 Review the configuration information. If you need to change an option, click **Edit** for that section.

Step 9 Click **Install This Configuration**.

What to do next

A *Next Steps* page should appear once the configuration installed. However, depending on the IP, host name, or DNS settings you configured during setup, you may lose connection to the appliance at this stage. If a "page not found" error is displayed in your browser, change the URL to reflect any new address settings and reload the page. Then continue with any post-setup tasks you wish to perform.

System Setup Wizard Reference Information

Network / System Settings

Property	Description
Default System Hostname	The system hostname is the fully-qualified hostname used to identify the appliance in the following areas: • the command line interface (CLI) • system alerts • end-user notification and acknowledgment pages • when forming the machine NetBIOS name when the Secure Web Appliance joins an Active Directory domain The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.
DNS Server(s)	• **Use the Internet's Root DNS Servers** – You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network. **Note** Internet Root DNS servers will not resolve local host names. If you need the appliance to resolve local host names you must use a local DNS server, or add the appropriate static entries to the local DNS using the CLI. • **Use these DNS Servers** – Provide address(es) for the local DNS server(s) that the appliance can use to resolve host names. See DNS Settings, on page 46 for more information about these settings.
NTP Server	The Network Time Protocol (NTP) server used to synchronize the system clock with other servers on the network or the Internet. The default is time.sco.cisco.com.
Time Zone	Provide time-zone information for location of the appliance; affects timestamps in message headers and log files.
Appliance Mode of Operation	• **Standard** – Used for standard on-premise policy enforcement. • **Cloud Web Security Connector** – Used primarily to direct traffic to Cisco's Cloud Web Security service for policy enforcement and threat defense. • **Hybrid Web Security** – Used in conjunction with Cisco's Cloud Web Security service for cloud and on-premise policy enforcement and threat defense. See Comparison of Modes of Operation, on page 2 for more information about these modes of operation.

Network / Network Context

Note When you use the Secure Web Appliance in a network that contains another proxy server, it is recommended that you place the Secure Web Appliance downstream from the proxy server, closer to the clients.

Property	Description
Is there another web proxy on your network?	Is there another proxy on your network, such that traffic must pass through it? it will be upstream of the Secure Web Appliance? If yes for both points, select the checkbox. This allows you to create a proxy group for one upstream proxy. You can add more upstream proxies later.
Proxy group name	A name used to identify the proxy group on the appliance.
Address	The hostname or IP address of the upstream proxy server.
Port	The port number of the upstream proxy server.

Related Topics

- Upstream Proxies, on page 16

Network / Cloud Connector Settings

Need to confirm page name and settings.

Setting	Description
Cloud Web Security Proxy Servers	The address of the Cloud Proxy Server (CPS), for example, proxy1743.scansafe.net .
Failure Handling	If AsyncOS fails to connect to a Cloud Web Security proxy, either **Connect directly** to the Internet, or **Drop requests**.
Cloud Web Security Authorization Scheme	Method for authorizing transactions: • Secure Web Appliance public-facing IPv4 address. • Authorization key included with each transaction. You can generate an authorization key within the Cisco Cloud Web Security Portal.

Network / Network Interfaces and Wiring

The IP address, network mask, and host name to use to manage the Secure Web Appliance and, by default, for proxy (data) traffic.

You can use the host name specified here when connecting to the appliance management interface (or in browser proxy settings if M1 is used for proxy data), but you must register it in your organization's DNS.

Setting	Description
Ethernet Port	(Optional) Check **Use M1 port for management only** if you want to use a separate port for data traffic. If you configure the M1 interface for management traffic only, you must configure the P1 interface for data traffic. You must also define different routes for management and data traffic. However, you can configure the P1 interface even when the M1 interface is used for both management and data traffic. You can enable and configure the P1 port only in the System Setup Wizard. If you want to enable the P2 interface, you must do this after finishing the System Setup Wizard.
IP Address / Netmask	The IP address and network mask to use when managing the Secure Web Appliance on this network interface.
Hostname	The host name to use when managing the Secure Web Appliance on this network interface.

Network / Layer 4 Traffic Monitor Wiring

Property	Description
Layer-4 Traffic Monitor	The type of wired connections plugged into the "T" interfaces: • **Duplex TAP.** The T1 port receives both incoming and outgoing traffic. • **Simplex TAP.** The T1 port receives outgoing traffic (from the clients to the Internet) and the T2 port receives incoming traffic (from the Internet to the clients). Cisco recommends using Simplex when possible because it can increase performance and security.

Network / Routes for Management and Data Traffic

Note If you enable "Use M1 port for management only", this section will have separate sections for management and data traffic; otherwise one joint section will be shown.

Property	Description
Default Gateway	The default gateway IP address to use for the traffic through the Management and Data interfaces.

Property	Description
Static Routes Table	Optional static routes for management and data traffic. Multiple routes can be added. • **Name** – A name used to identify the static route. • **Internal Network** – The IPv4 address for this route's destination on the network. • **Internal Gateway** – The gateway IPv4 address for this route. A route gateway must reside on the same subnet as the Management or Data interface on which it is configured.

Network / Transparent Connection Settings

Note By default, the Cloud Connector is deployed in transparent mode. which requires a connection to a Layer-4 switch, or a version 2 WCCP router.

Property	Description
Layer-4 Switch or No Device	Specifies that the Secure Web Appliance is connected to a layer 4 switch for transparent redirection, or that no transparent redirection device is used and clients will explicitly forward requests to the appliance.
WCCP v2 Router	Specifies that the Secure Web Appliance is connected to a version 2 WCCP-capable router. If you connect the appliance to a version 2 WCCP router, you must create at least one WCCP service. You can enable the standard service on this screen, or after the System Setup Wizard is finished, where you can also create multiple dynamic services. When you enable the standard service, you can also enable router security and enter a passphrase. The passphrase used here must be used all appliances and WCCP routers within the same service group. A standard service type (also known as the "web-cache" service) is assigned a fixed ID of zero, a fixed redirection method (by destination port), and a fixed destination port of 80. A dynamic service type allows you to define a custom ID, port numbers, and redirection and load balancing options.

Network /Administrative Settings

Property	Description
Administrator Passphrase	The passphrase used to access the Secure Web Appliance for administrative purposes.

Property	Description
Email System Alerts To	The email address to which the appliance sends systems alerts.
Send Email via SMTP Relay Host (optional)	The address and port for an SMTP relay host that AsyncOS can use to send system generated email messages. If no SMTP relay host is defined, AsyncOS uses the mail servers listed in the MX record.
AutoSupport	Specifies whether the appliance sends system alerts and weekly status reports to Cisco Customer Support.
SensorBase Network Participation	Specifies whether to participate in the Cisco SensorBase Network. If you participate, you can configure Limited or Standard (full) participation. Default is Standard. The SensorBase Network is a threat management database that tracks millions of domains around the world and maintains a global watch list for Internet traffic. When you enable SensorBase Network Participation, the Secure Web Appliance sends anonymous statistics about HTTP requests to Cisco to increase the value of SensorBase Network data.

Security / Security Settings

Option	Description
Global Policy Default Action	Specifies whether to block or monitor all web traffic by default after the System Setup Wizard completes. You can change this behavior later by editing the Protocols and User Agents settings for the Global Access Policy. The default setting is to monitor traffic.
L4 Traffic Monitor	Specifies whether the Layer-4 Traffic Monitor should monitor or block suspected malware by default after the System Setup Wizard completes. You can change this behavior later. The default setting is to monitor traffic.
Acceptable Use Controls	Specifies whether or not to enable Acceptable Use Controls. If enabled, Acceptable Use Controls allow you to configure policies based on URL filtering. They also provide application visibility and control, as well as related options such as safe search enforcement. The default setting is enabled.
Reputation Filtering	Specifies whether or not to enable Web Reputation filtering for the Global Policy Group. Web Reputation Filters is a security feature that analyzes web server behavior and assigns a reputation score to a URL to determine the likelihood that it contains URL-based malware. The default setting is enabled.

Option	Description
Malware and Spyware Scanning	Specifies whether to enable malware and spyware scanning using Webroot, McAfee, or Sophos. The default setting is that all three options are enabled. Most security services will be automatically enabled/disabled to match the services normally available for cloud policies. Similarly, policy-related defaults will not be applicable. At least one scanning option must be enabled. If any option is enabled, also choose whether to monitor or block detected malware. The default setting is to monitor malware. You can further configure malware scanning after you finish the System Setup Wizard.
Cisco Data Security Filtering	Specifies whether or not to enable Cisco Data Security Filters. If enabled, the Cisco Data Security Filters evaluate data leaving the network and allow you to create Cisco Data Security Policies to block particular types of upload requests. The default setting is enabled.

Upstream Proxies

The web proxy can forward web traffic directly to its destination web server or use routing policies to redirect it to an external upstream proxy.

- Upstream Proxies Task Overview, on page 16
- Creating Proxy Groups for Upstream Proxies, on page 16

Upstream Proxies Task Overview

Task	More Information
• Connect the external proxy upstream of the Cisco Secure Web Appliance.	Connect the Appliance, on page 5.
• Create and configure a proxy group for the upstream proxy.	Creating Proxy Groups for Upstream Proxies, on page 16.
• Create a routing policy for the proxy group to manage which traffic is routed to the upstream proxy.	Create Policies to Control Internet Requests

Creating Proxy Groups for Upstream Proxies

Step 1 Choose **Network > Upstream Proxies.**

Step 2 Click **Add Group**.

Step 3 Complete the Proxy Group settings.

Property	Description
Name	The name used to identify proxy groups on the appliance, such as in routing policies, for example.
Proxy Servers	The address, port and reconnection attempts (should a proxy not respond) for the proxy servers in the group. Rows for each proxy server can be added or deleted as required. **Note** You can enter the same proxy server multiple times to allow unequal load distribution among the proxies in the proxy group.
Load Balancing	The strategy that the web proxy uses to load balance requests between multiple upstream proxies. Choose from: • **None (failover)**. The Web Proxy directs transactions to one external proxy in the group. It tries to connect to the proxies in the order they are listed. If one proxy cannot be reached, the Web Proxy attempts to connect to the next one in the list. • **Fewest connections**. The Web Proxy keeps track of how many active requests are with the different proxies in the group and it directs a transaction to the proxy currently servicing the fewest number of connections. • **Hash based. Least recently used**. The Web Proxy directs a transaction to the proxy that least recently received a transaction if all proxies are currently active. This setting is similar to round robin except the Web Proxy also takes into account transactions a proxy has received by being a member in a different proxy group. That is, if a proxy is listed in multiple proxy groups, the “least recently used” option is less likely to overburden that proxy. • **Round robin**. The Web Proxy cycles transactions equally among all proxies in the group in the listed order. **Note** The Load Balancing option is dimmed until two or more proxies have been defined.
Failure Handling	Specifies the default action to take if all proxies in this group fail. Choose from: • **Connect directly.** Send the requests directly to their destination servers. • **Drop requests.** Discard the requests without forwarding them.

Step 4 Submit and commit your changes.

What to do next

- Creating a Policy

Network Interfaces

IP Address Versions

In Standard mode, Cisco Secure Web Appliance supports IPv4 and IPv6 addresses in most cases.

Note In Cloud Connector mode, Cisco Secure Web Appliance supports IPv4 only.

A DNS server may return a result with both an IPv4 and an IPv6 address. DNS settings include an IP Address Version Preference to configure AsyncOS behavior in these cases.

Interface/Service	IPv4	IPv6	Notes
M1 interface	Required	Optional	Use of IPv6 addresses requires an IPv6 routing table that defines the default IPv6 gateway. Depending on the network, you may also need to specify a static IPv6 route in the routing table.
P1 interface	Optional	Optional	If the P1 interface has an IPv6 address configured and the appliance uses split routing (separate management and data routes), then the P1 interface cannot use the IPv6 gateway configured on the Management route. Instead, specify an IPv6 gateway for the Data routing table.
P2 interface	Optional	Optional	—
Data services	Supported	Supported	—
Control and Management Services	Supported	Partially Supported	Images, for example custom logos on end-user notification pages, require IPv4.
AnyConnect Secure Mobility (MUS)	Supported	Not Supported	—

Related Topics

- Enabling or Changing Network Interfaces, on page 18
- DNS Settings, on page 46

Enabling or Changing Network Interfaces

- Add or modify interface IP addresses
- Change the Layer-4 Traffic Monitor wiring type
- Enable split routing of management and data traffic

Step 1 Choose **Network > Interfaces**.

Step 2 Click **Edit Settings**.

Step 3 Configure the Interface options.

Option	Description
Interfaces	Modify or add new IPv4 or IPv6 Address, Netmask, and Hostname details for the M1, P1, or P2 interfaces as required. • **M1** – AsyncOS requires an IPv4 address for the M1 (Management) port. In addition to the IPv4 address, you can specify an IPv6 address. By default, the Management interface is used to administer the appliance and Web Proxy (data) monitoring. However, you can configure the M1 port for management use only. • **P1** and **P2** – Use an IPv4 address, IPv6 address, or both for the Data ports. The Data interfaces are used for Web Proxy monitoring and Layer-4 Traffic Monitor blocking (optional). You can also configure these interfaces to support outbound services such as DNS, software upgrades, NTP, and traceroute data traffic. **Note** If the Management and Data interfaces are all configured, each must be assigned IP addresses on different subnets. **Note** When split routing is enabled, the Management interface cannot communicate with the Smart Licensing Portal. To register the Secure Web Appliance with the Smart Licensing Portal, choose a Data interface. **Note** When split routing is configured, Secure Web Appliance uses the data interface to contact the external DLP server, and the management interface is restricted to only the management traffic. This results in all DLP traffic being considered as data traffic instead of management traffic while routing traffic to the DLP server. For example, when there are two packet captures with P1 and M1 interfaces filtered by DLP addresses, the DLP traffic is found on both interfaces. It is because of the management interface that sends keepalive packets to the DLP servers and DLP traffic comes from data interfaces.
Separate Routing for Management Services	Check **Restrict M1 port to appliance management services only** to limit M1 to management traffic only, requiring use of a separate port for data traffic. **Note** When you use M1 for management traffic only, configure at least one data interface, on another subnet, for proxy traffic. Define different routes for management and data traffic.
Appliance Management Services	Enable/disable use of, and specify a default port number for, the following network protocols: • **FTP** – Disabled by default. • **SSH** • **HTTP** • **HTTPS** Also, you can enable/disable redirection of HTTP traffic to HTTPS.

Step 4 Submit and commit your changes.

What to do next

If you added an IPv6 address, add an IPv6 routing table.

Related Topics

- Connect the Appliance, on page 5.
- IP Address Versions, on page 18
- Configuring TCP/IP Traffic Routes, on page 33

Network Interface Card Configuration

This topic contains the following sections:

Media Settings on Ethernet Interfaces

You can access the media settings for the ethernet interfaces using the **etherconfig** command. Each ethernet interface is listed with its current setting. By selecting the interface, the applicable media settings are displayed.

Using etherconfig to Edit Media Settings on the Ethernet Interfaces

Use the **etherconfig** command to set the duplex settings (full/half) and the speed (10/100/1000 Mbps) of the ethernet interfaces. By default, interfaces automatically select the media settings; which you can override.

Note If you have completed the GUI's System Setup Wizard (or the Command Line Interface **systemsetup** command) as described in the Connect, Install, and Configure topic and committed the changes, the default ethernet interface settings should already be configured on your appliance.

Example of Editing Media Settings

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
[]> MEDIA
Ethernet interfaces:
1. Management (Autoselect: <1000baseT full-duplex>) 00:50:56:87:a6:46
2. P1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
```

```
3. P2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:6a:42
4. T1 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:1c:3f
5. T2 (Autoselect: <1000baseT full-duplex>) 00:50:56:87:fc:01

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
```

Network Interface Card Pairing/Teaming

NIC pairing allows you to combine any two physical data ports to provide a backup Ethernet interface if the data path from the NIC to the upstream Ethernet port should fail. Basically, pairing configures the Ethernet interfaces so that there is a primary interface and a backup interface. If the primary interface fails (for example, if the carrier between the NIC and the upstream node is disrupted), the backup interface becomes active and an alert is sent. When the primary interface become available, this interface automatically becomes active. Within the documentation for this product, NIC pairing is synonymous with NIC teaming.

Note NIC pairing is not available on S170, S190 and S195 web gateways.

You can create more than one NIC pair, provided you have enough data ports. When creating pairs, you can combine any two data ports. For example:

- Data 1 and Data 2
- Data 3 and Data 4
- Data 2 and Data 3

Some web gateways contain a fiber optic network interface option. If available, you will see two additional ethernet interfaces (Data 3 and Data 4) in the list of available interfaces on these web gateways. In a heterogeneous configuration, these gigabit fiber optic interfaces can be paired with the copper (Data 1, Data 2, and Management) interfaces.

Secure Web Appliance does not support packet capture for the NIC paired interfaces. The packet capture will be applied only for the active interface. For example, if both P1 and P2 are paired, both P1 and P2 will not be configured in the user interface or the CLI.

NIC Pairing and VLANs

VLANs (see Increasing Interface Capacity Using VLANs) are allowed only on the primary interface.

NIC Pair Naming

When creating NIC pairs, you must specify a name for the pair. NIC pairs created in AsyncOS prior to version 4.5 will automatically receive the default name of ‘Pair 1’ following an upgrade.

Any alerts generated on NIC pairing will reference the specific NIC pair by its name.

NIC Pairing and Existing Listeners

If you enable NIC pairing on an interface that has listeners assigned to it, you are prompted to either delete, reassign, or disable all listeners assigned to the backup interface.

Enabling NIC Pairing using the etherconfig Command

Note NIC pairing is not available on S170, S190 and S195 web gateways.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
Choose the operation you want to perform:
- NEW - Create a new pairing.
[]> NEW
Please enter a name for this pair (Ex: "Pair 1"):
[]> DP1

1. P1
2. P2
Enter the name or number of the primary ethernet interface you wish bind to.
[]> 1

1. P2
2. T1
3. T2
Enter the name or number of the backup ethernet interface you wish to pair.
[]> 2

Paired interfaces:
1. DP1:
        Primary (P1)
        Backup (T1)

Choose the operation you want to perform:
- NEW - Create a new pairing.
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]>
example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:40:34 2020 MST
example.com> interfaceconfig


Currently configured interfaces:
```

```
1. Management (10.10.192.167/24 on Management: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]> NEW
Ethernet interface:
1. Management
2. DP1
3. P2
[1]> 2
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[]> 10.10.102.66
Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 27
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Hostname:
[]> example.com
Currently configured interfaces:
1. Management (10.10.192.167/24 on Management: example.com)
2. P1 (10.10.102.66/27 on DP1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
- DETAILS - Show details of an interface.
[]>
example.com>example.com> commit
Warning: In order to process these changes, the proxy
process will restart after Commit. This will cause a brief
interruption in service. Additionally, the authentication
cache will be cleared, which might require some users to
authenticate again.
Warning: Processing of network configuration changes might
cause a brief interruption in network availability.
Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Thu Sep 24 01:43:18 2020 MST
example.com> exitexample.com:rtestuser 53] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
```

```
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:fc:01
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet6 fe80::250:56ff:fe87:a646%lagg0 prefixlen 64 scopeid 0x7
        inet 10.10.102.66 netmask 0xfffffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        groups: lagg
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
example.com:rtestuser 54]
```

Bringing Down the P1 Interface

P1 and T1 are paired and named as DP1. By bringing P1 down, T1 will become active. In the following example, look for the lagg0 interface.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> PAIRING
Paired interfaces:
1. DP1:
        Backup (T1) Standby, Link is up
        Primary (P1) Active, Link is up
2. DP2:
        Backup (T2) Standby, Link is up
        Primary (P2) Active, Link is up

Choose the operation you want to perform:
- DELETE - Delete a pairing.
- STATUS - Refresh status.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
```

```
[]>
example.com>
example.com> exit

example.com:rtestuser 115] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
```

```
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 116]
example.com:rtestuser 116] ifconfig nic1 down
example.com:rtestuser 117] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
```

```
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=1<MASTER>
        laggport: nic3 flags=4<ACTIVE>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 118]
```

Bringing Up the P1 Interface

```
example.com:rtestuser 118] ifconfig nic1 up
example.com:rtestuser 119] ifconfig
nic0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:a6:46
        hwaddr 00:50:56:87:a6:46
        inet 10.10.192.167 netmask 0xffffff00 broadcast 10.10.192.255
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:1c:3f
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        hwaddr 00:50:56:87:6a:42
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic3: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        hwaddr 00:50:56:87:dd:89
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
nic4: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
```

```
        hwaddr 00:50:56:87:fc:01
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=600003<RXCSUM,TXCSUM,RXCSUM_IPV6,TXCSUM_IPV6>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x6
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
bridge0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 00:50:56:87:dd:89
        nd6 options=1<PERFORMNUD>
        id 00:00:00:00:00:00 priority 32768 hellotime 2 fwddelay 15
        maxage 20 holdcnt 6 proto rstp maxaddr 2000 timeout 1200
        root id 00:00:00:00:00:00 priority 32768 ifcost 0 port 0
        member: nic4 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 5 priority 128 path cost 20000
        member: nic3 flags=942<DISCOVER,PRIVATE,AUTOEDGE,AUTOPTP>
                ifmaxaddr 0 port 4 priority 128 path cost 20000
lagg0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:1c:3f
        inet 10.10.102.66 netmask 0xfffffe0 broadcast 10.10.102.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic1 flags=5<MASTER,ACTIVE>
        laggport: nic3 flags=0<>
lagg1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 00:50:56:87:6a:42
        inet6 fe80::250:56ff:fe87:a646%lagg1 prefixlen 64 scopeid 0x9
        inet 10.10.166.66 netmask 0xfffffe0 broadcast 10.10.166.95
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet autoselect
        status: active
        laggproto failover lagghash l2,l3,l4
        laggport: nic2 flags=5<MASTER,ACTIVE>
        laggport: nic4 flags=0<>
example.com:rtestuser 120]
example.com:rtestuser 120]
```

Guidelines for Configuring NIC Pairing

M2, Data1, and Data2 cannot be used as primary or secondary or configured with an IP address.

Table 1:

Ports	Configured as IP Address	Action	What to do?	Split Routing Enabled	
				Primary	Secondary
P1 (Proxy)	Yes	Enabled	Connect P1 to the network for both incoming and outgoing traffic.	You can select P1 as primary for NIC Pairing **Note** If you select P2 as primary then you must delete the IP address for the P1.	P2, T1, T2
P1 + P2 (Proxy)	Yes	Enabled	Connect P1 to the internal network and P2 to the internet.	If you select P2 as primary and P1 as secondary, then you must delete the IP address for the P1. You will be prompted during the NIC pairing to delete the IP.	T1, T2
T1 (Traffic monitor)	No	Duplex Tap	One cable for all incoming and outgoing traffic.	NA	NA
T1 + T2 (Traffic monitor)	Yes	Simple Tap	One cable for all packets destined for the internet (T1) and one cable for all packets coming from the internet (T2).	NA	NA

Note If you choose to delete the IP for P1, then P1 will not be configured under split routing. When IP address is assigned for P2 or for the created NIC pair, then Split routing is enabled with only P2 configured. Link Aggregation (LAGG) interface is not shown till IP address is not assigned to the primary (p2) or NIC pair. Once the IP address is assigned to the primary (p2) or the NIC pair, LAGG interface is created.

Configuring Failover Groups for High Availability

Using the Common Address Redundancy Protocol (CARP), the Secure Web Appliance enable multiple hosts on your network to share an IP address, providing IP redundancy to ensure high availability of services provided by those hosts.

Failover is available only for the proxy service. The proxy automatically binds to the failover interface when the failover group is created. Thus, if the proxy goes down for any reason, failover is triggered.

In CARP, there are three states for a host:

- primary - there can only be one primary host in each failover group
- backup
- init

The primary host in the CARP failover group sends regular advertisements to the local network so that the back-up hosts know it is still alive. (This advertisement interval is configurable on the Secure Web Appliance). If the back-up hosts do not receive an advertisement from the primary for the specified period of time (because the proxy is down, or the Secure Web Appliance has gone down, or it is disconnected from the network), then failover is triggered and one of the backups will take over the duties of primary.

The advertisements from the primary Secure Web Appliance do not reach the remaining back-up hosts in the following conditions:

- Network/Interface Unavailability
- OS Health and Availability

Note Disable Data-Plane IP Learning in the Application Centric Infrastructure (ACI) to use the Secure Web Appliance High Availability feature.

Note You cannot use High Availability as a load balancing method between appliances. Use either WCCP or a hardware load balancer to load balance the traffic between devices.

The following are the configurations that causes high availability switchovers:

- Add or remove or update the Authentication Realm
- Add or remove or update the ISE settings

- Add or update the HTTPS certificate
- Update the log level (proxy log)
- Update the transparent redirection setting
- Enable or disable or update the FTP proxy
- Enable or disable or update the SOCKS proxy
- Add or modify the PAC file
- Add or remove the interface from the appliance
- Add or update failover groups
- Enable or disable Upstream proxy
- Enable or disable WTT (web traffic tap)

Add Failover Group

Before you begin

- Identify a virtual IP address that will be used exclusively for this failover group. Clients will use this IP address to connect to the failover group in explicit forward proxy mode.
- Configure all Appliances in the failover group with identical values for the following parameters:
  - Failover Group ID
  - Hostname
  - Virtual IP Address
- If you are configuring this feature on a virtual appliance, ensure that the virtual switch and the virtual interfaces specific to each appliance are configured to use promiscuous mode. For more information, see the documentation for your virtual hypervisor.

Step 1 Choose **Network > High Availability**.

Step 2 Click **Add Failover Group**.

Step 3 Enter a **Failover Group ID** in the range 1 to 255.

Step 4 (Optional) Enter a Description.

Step 5 Enter the **Hostname**, for example www.example.com.

Step 6 Enter the **Virtual IP Address and Netmask**, for example 10.0.0.3/24 (IPv4) or 2001:420:80:1::5/32 (IPv6).

Step 7 Choose an option from the **Interface** menu. The **Select Interface Automatically** option will select the interface based on the IP address you provided.

Note If you do not select the **Select Interface Automatically** option, you must choose an interface in the same subnet as the virtual IP address you provided.

Step 8 Choose the priority. Click **Primary** to set the priority to 255. Alternatively, select **Backup** and enter a priority between 1 (lowest) and 254 in the **Priority** field.

Step 9 (Optional). To enable security for the service, select the **Enable Security for Service** check box and enter a string of characters that will be used as a shared secret in the **Shared Secret** and **Retype Shared Secret** fields.

Note The shared secret, virtual IP, and failover group ID must be the same for all appliances in the failover group.

Step 10 Enter the delay in seconds (1 to 255) between hosts advertising their availability in the **Advertisement Interval** field.

Step 11 Submit and commit your changes.

What to do next

Related Topics

- Failover Problems

Edit High Availability Global Settings

Step 1 Choose **Network > High Availability**.

Step 2 In the **High Availability Global Settings** area, click **Edit Settings**.

Step 3 In the **Failover Handling** menu, choose an option.

- **Preemptive**—The highest priority host will assume control when available.
- **Non-preemptive**—The host in control will remain in control even if a higher priority host becomes available.

Step 4 Click **Submit**. Alternatively, click **Cancel** to abandon your changes.

View Status of Failover Groups

Choose **Network > High Availability**. The Failover Groups area displays the current fail-over group. You can click **Refresh Status** to update the display. You can also view fail-over details by choosing **Network > Interfaces** or **Report > System Status**.

Using the P2 Data Interface for Web Proxy Data

By default, the web proxy does not listen for requests on P2, even when enabled. However, you can configure P2 to listen for web proxy data.

Note If you enable P2 to listen for client requests using the `advancedproxyconfig > miscellaneous` CLI command, you can choose whether to use P1 or P2 for outgoing traffic. To use P1 for outgoing traffic, change the Default Route for data traffic to specify the next IP address that the P1 interface is connected to.

Before you begin

Enable P2 (you must also enable P1 if not already enabled) (see Enabling or Changing Network Interfaces, on page 18).

Step 1 Access the CLI.

Step 2 Use the `advancedproxyconfig` > `miscellaneous` commands to access the required area

```
example.com> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
```

Step 3 []> **miscellaneous**

Step 4 Press **Enter** past each question until the question:

```
Do you want proxy to listen on P2?
```

Enter '**y**' for this question.

Step 5 Press **Enter** past the remaining questions.

Step 6 Commit your changes.

What to do next

Related Topics

- Connect the Appliance, on page 5.
- Configuring TCP/IP Traffic Routes, on page 33.
- Configuring Transparent Redirection, on page 36

Configuring TCP/IP Traffic Routes

Routes are used for determining where to send (or route) network traffic. The Secure Web Appliance routes the following kinds of traffic:

- **Data traffic.** Traffic the Web Proxy processes from end users browsing the web.
- **Management traffic.** Traffic created by managing the appliance through the web interface and traffic the appliance creates for management services, such as AsyncOS upgrades, component updates, DNS, authentication, and more.

By default, both types of traffic use the routes defined for all configured network interfaces. However, you can choose to split the routing, so that management traffic uses a management routing table and data traffic uses a data routing table. Both types of traffic split are split as follows:

Management Traffic	Data Traffic
• WebUI • SSH • SNMP • NTLM authentication (with domain controller) • Syslogs • FTP push • DNS (configurable) • Update/Upgrade/Feature Key (configurable)	• HTTP • HTTPS • FTP • WCCP negotiation • ICAP request with external DLP server • DNS (configurable) • Update/Upgrade/Feature Key (configurable) • LDAP/NTLM authentication with domain controller (configurable)

The number of sections on the **Network** > **Routes** page is determined by whether or not split routing is enabled:

- **Separate route configuration sections for Management and Data traffic** (split routing enabled). When you use the Management interface for management traffic only (**Restrict M1 port to appliance management services only** is enabled), then this page includes two sections to enter routes, one for management traffic and one for data traffic.
- **One route configuration section for all traffic** (split routing not enabled). When you use the Management interface for both management and data traffic (**Restrict M1 port to appliance management services only** is disabled), then this page includes one section to enter routes for all traffic that leaves the Secure Web Appliance, both management and data traffic.

Note A route gateway must reside on the same subnet as the Management or Data interface on which it is configured. If multiple data ports are enabled, the web proxy sends out transactions on the data interface that is on the same network as the default gateway configured for data traffic.

Outbound Services Traffic

The Secure Web Appliance also uses the management and data interfaces to route outbound traffic for services such as DNS, software upgrades, NTP, and traceroute data traffic.You configure this for each service individually, by choosing the route it uses for outbound traffic. By default, the management interface is used for all services.

Related Topics

- To enable split routing of management and data traffic, see Enabling or Changing Network Interfaces, on page 18.

Modifying the Default Route

Step 1 Choose **Network > Routes**.

Step 2 Click on **Default Route** in the Management or Data table as required (or the combined Management/Data table if split routing is not enabled).

Step 3 In the Gateway column, enter the IP address of the computer system on the next hop of the network connected to the network interface you are editing.

Step 4 Submit and commit your changes.

Adding a Route

Step 1 Choose **Network > Routes**.

Step 2 Click the **Add Route** button corresponding to the interface for which you are creating the route.

Step 3 Enter a Name, Destination Network, and Gateway.

Step 4 Submit and commit your changes.

Saving and Loading Routing Tables

Choose **Network > Routes**.

To save a route table, click **Save Route Table** and specify where to save the file.

To load a saved route table, click **Load Route Table**, navigate to the file, open it, and submit and commit your changes.

Note When the destination address is on the same subnet as one of the physical network interfaces, AsyncOS sends data using the network interface with the same subnet. It does not consult the routing tables.

Deleting a Route

Step 1 Choose **Network > Routes**.

Step 2 Check the checkbox in the Delete column for the appropriate route.

Step 3 Click **Delete** and confirm**.**

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Enabling or Changing Network Interfaces, on page 18.

Configuring Transparent Redirection

Specifying a Transparent Redirection Device

Before you begin

Connect the appliance to a Layer-4 switch or a WCCP v2 router.

Step 1 Choose **Network > Transparent Redirection**.

Step 2 Click **Edit Device**.

Step 3 Choose the type of device that transparently redirects traffic to the appliance from the Type drop-down list: **Layer 4 Switch or No Device** or **WCCP v2 Router**.

Step 4 Submit and commit your changes.

Step 5 For WCCP v2 devices, complete these additional steps:

a) Configure the WCCP device using device documentation.

b) On the Secure Web Appliance's Transparent Redirection page, click **Add Service** to add a WCCP service, as described in Adding and Editing a WCCP Service, on page 38.

c) If IP spoofing is enabled on the appliance, create a second WCCP service.

What to do next

Related Topics

- Connect the Appliance, on page 5.
- Configuring WCCP Services, on page 37.

Using An L4 Switch

If you are using a Layer 4 switch for transparent redirection, depending how it is configured, you may need to configure a few additional options on the Secure Web Appliance.

- Generally, do not enable IP Spoofing; if you spoof upstream IP addresses you may create an asynchronous routing loop.
- On the Edit Web Proxy Settings page (Security Services > Web Proxy), check **Enable Identification of Client IP Addresses using X-Forwarded-For** in the **Use Received Headers** section (Advanced Settings). Then add one or more egress IP addresses to the **Trusted Downstream Proxy or Load Balancer** list.
- Optionally, you can use the CLI command `advancedproxyconfig > miscellaneous` to configure the following proxy-related parameters as necessary:
  - `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)?` – Enter Y if you want to allow the Secure Web Appliance to respond to health checks.

- `Would you like proxy to perform dynamic adjustment of TCP receive window size?` – Use the default Y in most cases; enter N if you have another proxy device upstream of the Secure Web Appliance.
- `Do you want to pass HTTP X-Forwarded-For headers?` – No need unless there is a requirement upstream for X-Forwarded-For (XFF) headers.
- `Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?` – To aid in troubleshooting, you can enter Y; client IP addresses will be displayed in the access logs.
- `Would you like the proxy to use client IP addresses from X-Forwarded-For headers?` Again, to aid policy configuration and reporting, you can enter Y.

- If you are using X-Forwarded-For (XFF) headers, add `%f` to the Access Logs subscription in order to log the XFF headers. For the W3C Logs format, add `cs(X-Forwarded-For)`.

Configuring WCCP Services

A WCCP service is an appliance configuration that defines a service group to a WCCP v2 router. It includes information such as the service ID and ports used. Service groups allow a web proxy to establish connectivity with a WCCP router and to handle redirected traffic from the router.

If WCCP proxy health checking is enabled, the Secure Web Appliance's WCCP daemon sends a proxy health check message (xmlrpc client request) to the xmlrpc server running on the Web proxy every 10 seconds. If the proxy is up and running, the WCCP service receives a response from the proxy and the Secure Web Appliance sends a WCCP "here I am" (HIA) message to the specified WCCP-enabled routers every 10 seconds. If the WCCP service doesn't receive a reply from the proxy, then HIA messages are not sent to the WCCP routers.

After a WCCP router misses three consecutive HIA messages, the router removes the Secure Web Appliance from its service group and traffic is no longer forwarded to the Secure Web Appliance.

You can use the CLI command `advancedproxyconfig` > `miscellaneous` > `Do you want to enable WCCP proxy health check?` to enable and disable the proxy health check messages; the health check is disabled by default.

Note The WCCPv2 service works with the IPv4 and IPv6 networks. A maximum of 15 service groups can be configured on a single appliance. Each service group on the WCCP router can contain up to 32 appliances. The WCCPv2 service is also used for the Load Balancing mechanism to reduce content engine overloading and data blocking.

Note Configuring WCCP and High Availability on the same appliance is not supported. If configured, Secure Web Appliancewill not function as expected.

- About WCCP Load Balancing, on page 38
- Adding and Editing a WCCP Service, on page 38
- Creating WCCP Services for IP Spoofing, on page 41

About WCCP Load Balancing

The **Assignment Weight** parameter in the WCCP service definition is used to adjust the load on this Secure Web Appliance when it is operating as member of a WCCP pool, or service group. This weighting represents the proportion of total WCCP traffic that can be sent to this Secure Web Appliance for processing.

Assignment weighting adjustment is required only when different types of gateway appliances are members of the same WCCP pool and you need to divert more of the traffic to the stronger appliances.

Note All Secure Web Appliances that are members of a WCCP pool must be running a version of AsyncOS that supports assignment weighting to benefit from WCCP load balancing.

Note WCCP load balances transparent traffic for up to 32 appliances. It balances the traffic flow based on hash or mask and they are weighted when several appliance models exist in the network. Without any downtime, you can add and remove devices from the service pool. However, if you are using or plan to use more than 8 appliances, we recommend having a dedicated load balancer.

See Adding and Editing a WCCP Service, on page 38 for more information about the **Assignment Weight** parameter.

Adding and Editing a WCCP Service

Before you begin

Configure the appliance to use a WCCP v2 Router (see Specifying a Transparent Redirection Device, on page 36).

Step 1 Choose **Network > Transparent Redirection**.

Step 2 Click **Add Service**, or, to edit a WCCP service, click the name of the WCCP service in the Service Profile Name column.

Step 3 Configure the WCCP options as described:

WCCP Service Option	Description
Service Profile Name	The name for the WCCP service. **Note** If you leave this empty and choose a standard service (see below), the name ‘web_cache’ is automatically assigned here.

WCCP Service Option	Description
Service	The service group type for the router. Choose from: **Standard service.** This service type is assigned a fixed ID of zero, a fixed redirection method of *by destination port,* and a fixed destination port of 80. You can create one standard service only. If a standard service already exists on the appliance, this option is dimmed. **Dynamic service.** This service type allows you to define a custom ID, port numbers, and redirection and load balancing options. Enter the same parameters when creating the service on the WCCP router as you entered for the dynamic service. If you create a dynamic service, enter the following information: • **Service ID.** You can enter any number from 0 to 255 in the Dynamic Service ID field. However, note that you can configure no more than 15 service groups on this appliance. • **Port number(s).** Enter up to eight port numbers for traffic to redirect in the Port Numbers field. • **Redirection basis.** Choose to redirect traffic based on the source or destination port. Default is destination port. **Note** To configure Native FTP with transparent redirection and IP spoofing, choose Redirect based on source port (return path) and set the source port to 13007. • **Load balancing basis.** When the network uses multiple Secure Web Appliance, you can choose how to distribute packets among the appliances. You can distribute packets based on the server or client address. When you choose client address, packets from a client always get distributed to the same appliance. Default is server address.
Router IP Addresses	The IPv4 or IPv6 address for one or more WCCP enabled routers. Use each router's unique IP; you cannot enter a multicast address. You cannot mix IPv4 and IPv6 addresses within a service group.
Router Security	Check **Enable Security for Service** to require a passphrase for this service group. If enabled, every appliance and WCCP router that uses the service group must use the same passphrase. Provide and confirm the passphrase to use.

WCCP Service Option	Description
Advanced	**Load-Balancing Method.** This determines how the router performs load balancing of packets among multiple Secure Web Appliance. Choose from: • **Allow Mask Only.** WCCP routers make decisions using hardware in the router. This method can increase router performance over the hash method. Not all WCCP routers support mask assignment, however. (IPv4 only.) • **Allow Hash Only.** This method relies on a hash function to make redirection decisions. This method can be less efficient than the mask method, but may be the only option the router supports. (IPv4 and IPv6.) • **Allow Hash or Mask**. Allows AsyncOS to negotiate a method with the router. If the router supports mask, then AsyncOS uses masking, otherwise hashing is used. **Mask Customization.** If you select Allow Mask Only or Allow Hash or Mask, you can customize the mask or specify the number of bits: • **Custom mask (max 6 bits)**. You can specify the mask. The web interface displays the number of bits associated with the mask you provide. You can use up to five bits for an IPv4 router, or six bits for an IPv6 router. • **System generated mask.** You can let the system generate a mask for you. Optionally, you can specify the number of bits for the system-generated mask, between one and five bits. **Assignment Weight** – The WCCP weighting for this Secure Web Appliance; valid values are zero to 255. This weighting represents the proportion of total traffic that can be sent to this Secure Web Appliance for processing as member of a WCCP service group. A value of zero means this Secure Web Appliance will be a part of the service group, but it will not receive any redirected traffic from the router. See About WCCP Load Balancing, on page 38 for more information. **Forwarding method.** This is the method by which redirected packets are transported from the router to the web proxy. **Return Method.** This is the method by which redirected packets are transported from the web proxy to the router.

WCCP Service Option	Description
	Both the forwarding and return methods use one of the following method types: • **Layer 2 (L2).** This redirects traffic at layer 2 by replacing the packet's destination MAC address with the MAC address of the target web proxy. The L2 method operates at hardware level and typically offers the best performance. Not all WCCP routers support L2 forwarding, however. In addition, WCCP routers only allow L2 negotiation with a directly (physically) connected Secure Web Appliance. • **Generic Routing Encapsulation (GRE)**. This method redirects traffic at layer 3 by encapsulating the IP packet with a GRE header and a redirect header. GRE operates at software level, which can impact performance. • **L2 or GRE**. With this option, the appliance uses the method that the router says it supports. If both the router and appliance support L2 and GRE, the appliance uses L2. If the router is not directly connected to the appliance, you must choose GRE.

Step 4 Submit and commit your changes.

Creating WCCP Services for IP Spoofing

Step 1 If you have enabled IP spoofing on the web proxy, create two WCCP services. Create a standard WCCP service, or create a dynamic WCCP service that redirects traffic based on destination ports.

Step 2 Create a dynamic WCCP service that redirects traffic based on source ports.

Use the same port numbers, router IP address, and router security settings as used for the service created in Step 1.

Note
- Cisco suggests using a service ID number from 90 to 97 for the WCCP service used for the return path (based on the source port).
- Configure spoofed IP addresses appropriately when you set WCCP load balancing methods '**Allow Mask Only**' or '**Allow Hash or Mask**' to distribute traffic to multiple appliances. Spoofed IP address configuration must ensure proper routing of traffic between the WCCP router and the Secure Web Appliance.

What to do next

Related Topics

- Web Proxy Cache.

Increasing Interface Capacity Using VLANs

You can configure one or more VLANs to increase the number of networks the Cisco Secure Web Appliance can connect to beyond the number of physical interfaces included.

VLANs appear as dynamic “Data Ports” labeled in the format of: “VLAN DDDD” where the “DDDD” is the ID and is an integer up to 4 digits long (VLAN 2, or VLAN 4094 for example). AsyncOS supports up to 30 VLANs.

A physical port does not need an IP address configured in order to be in a VLAN. The physical port on which a VLAN is created can have an IP that will receive non-VLAN traffic, so you can have both VLAN and non-VLAN traffic on the same interface.

VLANS can be created on the Management interface using M1, P1 for internal Data ports, and P2 for external Data ports.

Configuring and Managing VLANs

You can create, edit and delete VLANs via the `etherconfig` command. Once created, a VLAN can be configured via the `interfaceconfig` command in the CLI.

Note Whenever you make changes to a VLAN configuration, ensure to reboot the appliance.

Example 1: Creating a New VLAN

In this example, two VLANs are created (named VLAN 31 and VLAN 34) on the P1 port:

Note Do not create VLANs on the T1 or T2 interfaces.

Step 1 Access the CLI.

Step 2 Follow the steps shown.

```
example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- MTU - View and configure MTU.
[]> vlan
VLAN interfaces:
Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 34
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
```

```
1. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Management
2. P1
3. T1
4. T2
[1]> 2
VLAN interfaces:
1. VLAN   31 (P1)
2. VLAN   34 (P1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
```

Step 3 Commit your changes.

Example 2: Creating an IP Interface on a VLAN

In this example, a new IP interface is created on the VLAN 34 ethernet interface.

Note Making changes to an interface may close your connection to the appliance.

Step 1 Access the CLI.

Step 2 Follow the steps shown:

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]> new
IP Address (Ex: 10.10.10.10):
[]> 10.10.31.10
Ethernet interface:
1. Management
2. P1
3. VLAN 31
4. VLAN   34
[1]> 4
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>
Hostname:
```

```
[]> v.example.com
Currently configured interfaces:
1. Management (10.10.1.10/24 on Management: example.com)
2. P1 (10.10.0.10 on P1: example.com)
3. VLAN   34 (10.10.31.10 on VLAN  34: v.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
example.com> commit
```

Step 3 Commit your changes.

What to do next

Related Topics

- Enabling or Changing Network Interfaces, on page 18.
- Configuring TCP/IP Traffic Routes, on page 33.

Redirect Hostname and System Hostname

After running the System Setup Wizard, the System Hostname and the Redirect Hostname are the same. However, changing the system hostname using the `sethostname` command does not change the redirect hostname. Therefore the settings may have different values.

AsyncOS uses the redirect hostname for end-user notifications and acknowledgments.

The system hostname is the fully-qualified hostname used to identify the appliance in the following areas:

- The command line interface (CLI)
- System alerts
- When forming the machine NetBIOS name when the Secure Web Appliance joins an Active Directory domain.

The system hostname does not correspond directly to interface hostnames and is not used by clients to connect to the appliance.

Changing the Redirect Hostname

Step 1 In the web user interface, navigate to **Network**>**Authentication**.

Step 2 Click Edit Global Settings.

Step 3 Enter a new value for Redirect Hostname.

Changing the System Hostname

Step 1 Access the CLI.

Step 2 Use the `sethostname` command to change the name of the Secure Web Appliance:

```
example.com> sethostname

example.com> hostname.com

example.com> commit
...
hostname.com>
```

Step 3 Commit your changes.

Configuring SMTP Relay Host Settings

AsyncOS periodically sends system-generated email messages, such as notifications, alerts, and Cisco Customer Support requests. By default, AsyncOS uses information listed in the MX record on your domain to send email. However, if the appliance cannot directly reach the mail servers listed in the MX record, you must configure at least one SMTP relay host on the appliance.

Note If the Secure Web Appliance cannot communicate with the mail servers listed in the MX record or any of the configured SMTP relay hosts, it cannot send email messages and it writes a message in the log files.

You can configure one or more SMTP relay hosts. When you configure multiple SMTP relay hosts, AsyncOS uses the topmost available SMTP relay host. If an SMTP relay host is unavailable, it tries to use the one below it in the list.

Configuring an SMTP Relay Host

Step 1 Choose **Network > Internal SMTP Relay**.

Step 2 Click **Edit Settings**.

Step 3 Complete the Internal SMTP Relay settings.

Property	Description
Relay Hostname or IP Address	The hostname or IP address to use for the SMTP relay
Port	The port for connecting to the SMTP relay. If this property is left empty, the appliance uses port 25.

Property	Description
Routing Table to Use for SMTP	The routing table associated with an appliance network interface, either Management or Data, to use for connecting to the SMTP relay. Choose whichever interface is on the same network as the relay system.

Step 4 (Optional) Click **Add Row** to add additional SMTP relay hosts.

Step 5 Submit and commit your changes.

DNS Settings

AsyncOS for Web can use the Internet root DNS servers or your own DNS servers. When using the Internet root servers, you can specify alternate servers to use for specific domains. Since an alternate DNS server applies to a single domain, it must be authoritative (provide definitive DNS records) for that domain.

You can also specify secondary DNS name servers to resolve the queries not resolved by the primary name servers. Secondary DNS servers are not used as failover DNS servers. They are queried according to the priority, when primary DNS servers return errors specified in Editing DNS Settings, on page 47.

To prevent authentication failures, ensure that the Secure Web Appliance authentication redirect name is unique.

- Split DNS, on page 47
- Clearing the DNS Cache, on page 47
- Editing DNS Settings, on page 47

Guidelines and Limitations for Secure DNS

Note By default, Secure DNS is disabled.

If you enable Secure DNS:

- You must use FQDN with the hostname for the local and private domains.
- Ensure that you configure the DNS server with DNSSec because there is no backward compatibility. Failing to do so can result in invalid response with an unresolved hostname.
- The system logs do not display:
  - Server details of the internet root's DNS requests
  - Detailed information on the debug and trace logs
- CNAME is not cached.
- Invalid DNSSEC response is not cached.

- The DNS cache gets cleared when the secure DNS setting is changed from disabled to enabled, and vice-versa.
- Ensure to select **Load Network Settings** to load the Secure DNS configuration.

Split DNS

AsyncOS supports split DNS where internal servers are configured for specific domains and external or root DNS servers are configured for other domains. If you are using your own internal server, you can also specify exception domains and associated DNS servers.

Clearing the DNS Cache

Before you begin

Be aware that using this command might cause a temporary performance degradation while the cache is repopulated.

Step 1 Choose **Network > DNS**.

Step 2 Click **Clear DNS Cache**.

Editing DNS Settings

Step 1 Choose **Network > DNS**

Step 2 Click **Edit Settings**.

Step 3 Configure the DNS settings as required.

Property	Description
Primary DNS Servers	**Use these DNS Servers.** The local DNS server(s) that the appliance can use to resolve hostnames. **Alternate DNS servers Overrides (Optional)**. Authoritative DNS servers for particular domains **Use the Internet's Root DNS Servers.** You can choose to use the Internet root DNS servers for domain name service lookups when the appliance does not have access to DNS servers on your network. **Note** Internet Root DNS servers will not resolve local hostnames. If you need the appliance to resolve local hostnames you must use a local DNS server or add the appropriate static entries to the local DNS using the Command Line Interface. This is required for accessing the new web interface as well.

Property	Description
Secondary DNS Servers	The secondary DNS server(s) that the appliance can use to resolve hostnames not resolved by the primary name servers. **Note** The secondary DNS servers receive host name queries when the primary DNS servers return the following errors: • No Error, no answer section received. • Server failed to complete request, no answer section. • Name Error, no answer section received. • Function not implemented. • Server Refused to Answer Query.
Routing Table for DNS Traffic	Specifies which interface the DNS service will route traffic through.
IP Address Version Preference	When a DNS server provides both an IPv4 and an IPv6 address, AsyncOS uses this preference to choose the IP address version. **Note** AsyncOS does not honor the version preference for transparent FTP requests.
Secure DNS	Check the **Secure DNS** check box to validate the authentication of DNS response received from the DNS server. **Note** Enabling Secure DNS increases the resolution time.
Wait Before Timing out Reverse DNS Lookups	The wait time in seconds before timing out non-responsive reverse DNS lookups.
Domain Search List	A DNS domain search list used when a request is sent to a bare hostname (with no '.' character). The domains specified will each be attempted in turn, in the order entered, to see if a DNS match for the hostname plus domain can be found.

Step 4 Submit and commit your changes.

What to do next

Related Topics

- Configuring TCP/IP Traffic Routes, on page 33
- IP Address Versions, on page 18

Troubleshooting Connect, Install, and Configure

- Failover Problems
- Upstream Proxy Does Not Receive Basic Credentials

- Client Requests Fail Upstream Proxy
- Maximum Port Entries