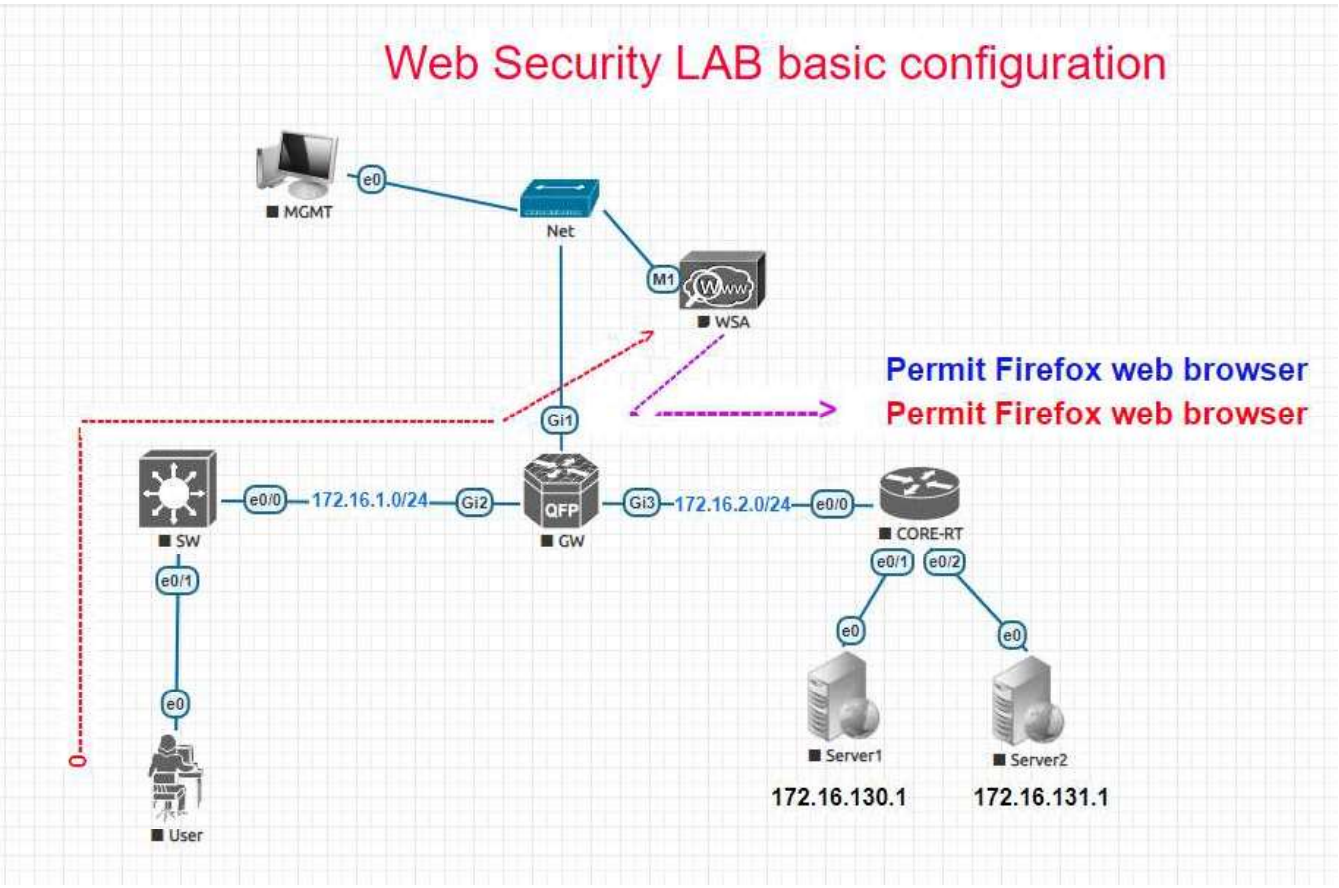


III. Question:

1. Your configuration should meet the following requirements:

- Traffic should be redirected to WSA at 192.168.1.2
- WCCP communication between R2 and WSA should be authenticated using password "cisco"
- Any traffic filtering applied should be network and host specific for the HTTP port 80
- Forwarding and Return Method for redirection should be GRE only.

2. Your configuration should meet the following requirements:

   HTTP traffic at port 80 originated from 172.16.1.0/24 network directed to server1 and server2 should be allowed if FireFox as a browser is used but dropped if originated from the Chorme Explorer, all the other traffic should be allowed.

   Identification Profile 1:

   - Name: Monitor Profile
   - Check for source 172.16.1.0/24
   - Check for browser Type-Version: FireFox-Any

   Identification Profile 2:

   - Name: Block Profile
   - Check for source 172.16.1.0/24
   - Check for browser Type-Version: Chrome-Any

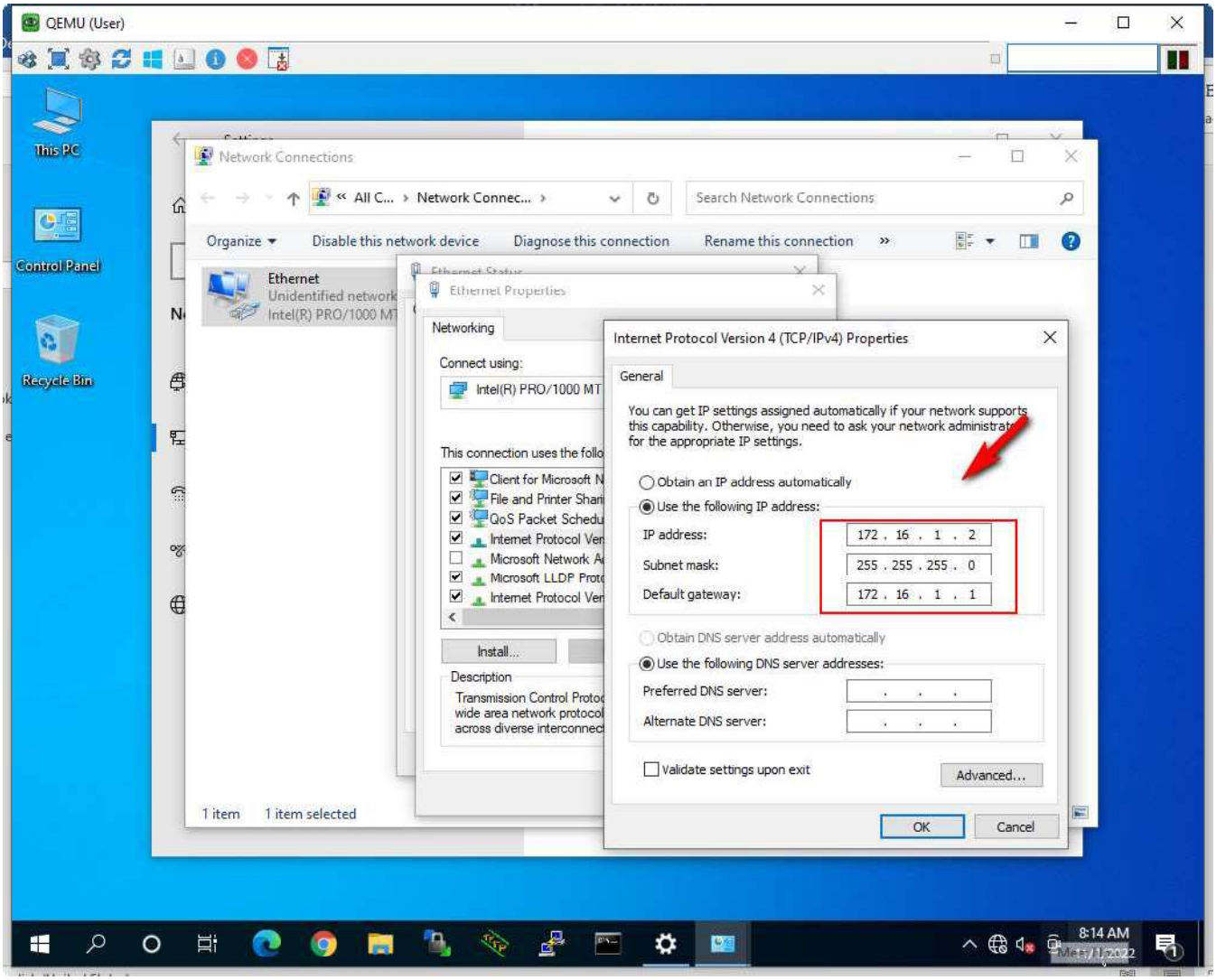
No	Device	IP mgmt.	account
1	WSA	192.168.1.2	admin/ironport
2	MGMT window 10	192.168.1.2	user/Test123
3	Internet |	172.16.130.1 172.16.131.1	user/Test123

IV. Solution:

1. Configure User Client

Windows 10

```
IP 172.16.1.2/24 sudo route add
default GW 172.16.1.1
```



2. WSA Configuration

- Step 1: download and add license WSA. Please flow this guideline:

https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html

- Step 2: initial setup. Please flow this guide

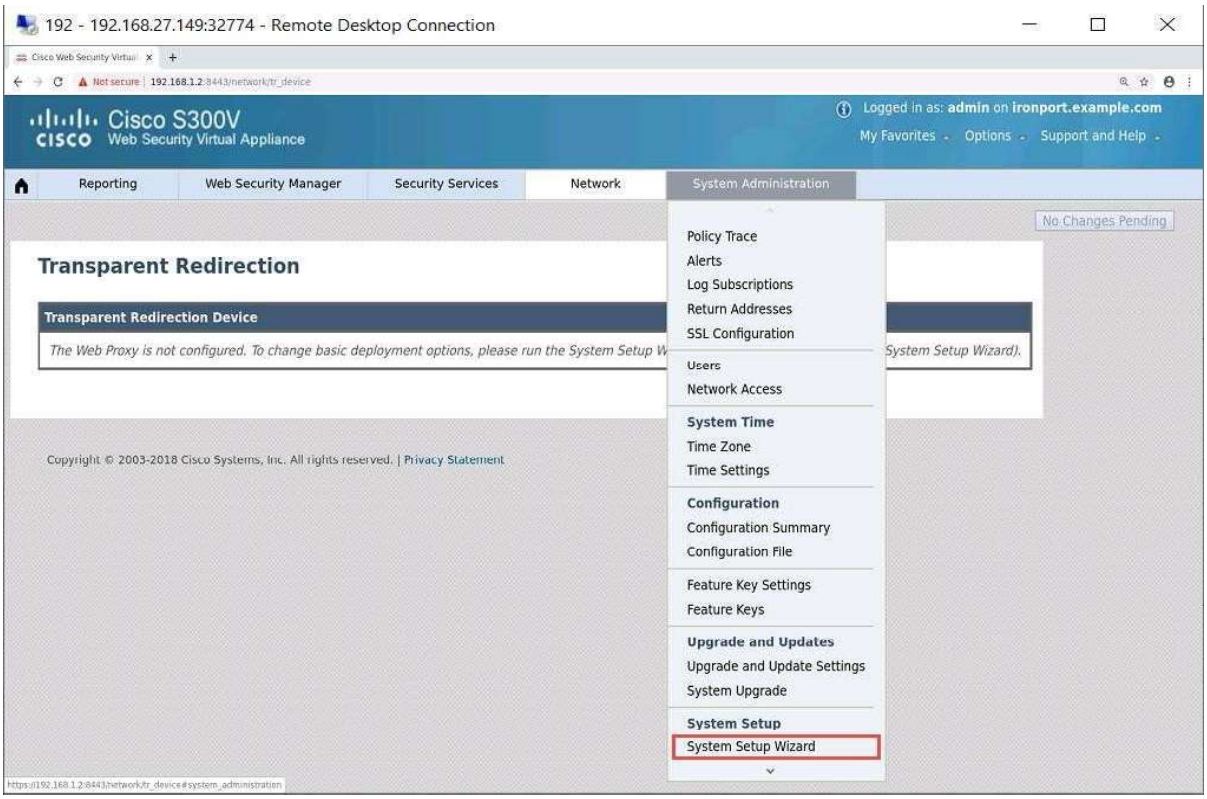
Click to WSA login with default password: admin/ironport

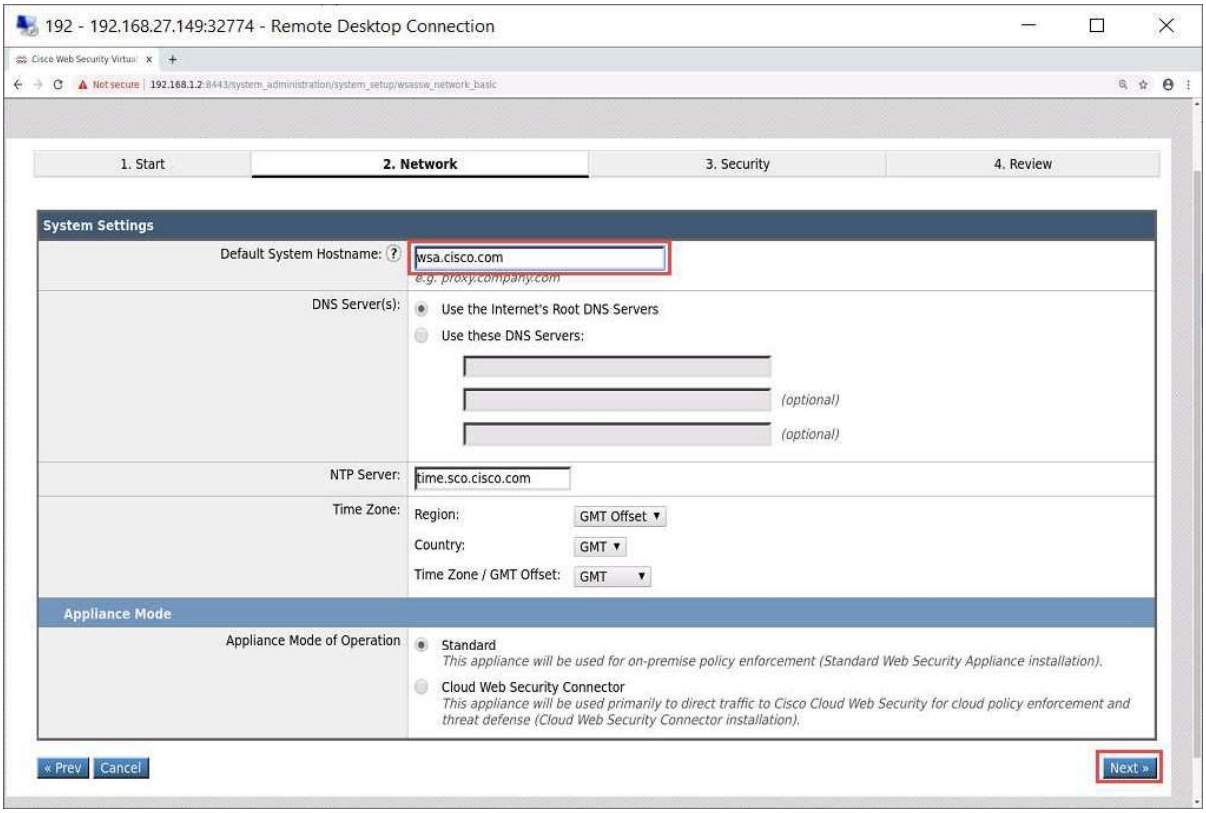
```
wsa.cisco.com> interfaceconfig


Currently configured interfaces:
1. Management (192.168.1.2/24 on Management: mgmt.wsa.cisco.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.
[]> EDIT

Enter the number of the interface you wish to edit.
[]> 1

Would you like to configure an IPv4 address for this interface (y/n)?
[Y]>

IPv4 Address (Ex: 192.168.1.2 ):
[192.168.1.2]> 192.168.1.2

Netmask (Ex: "24", "255.255.255.0" or "0xffffff00"):
[24]> 24

Enter then commit
```

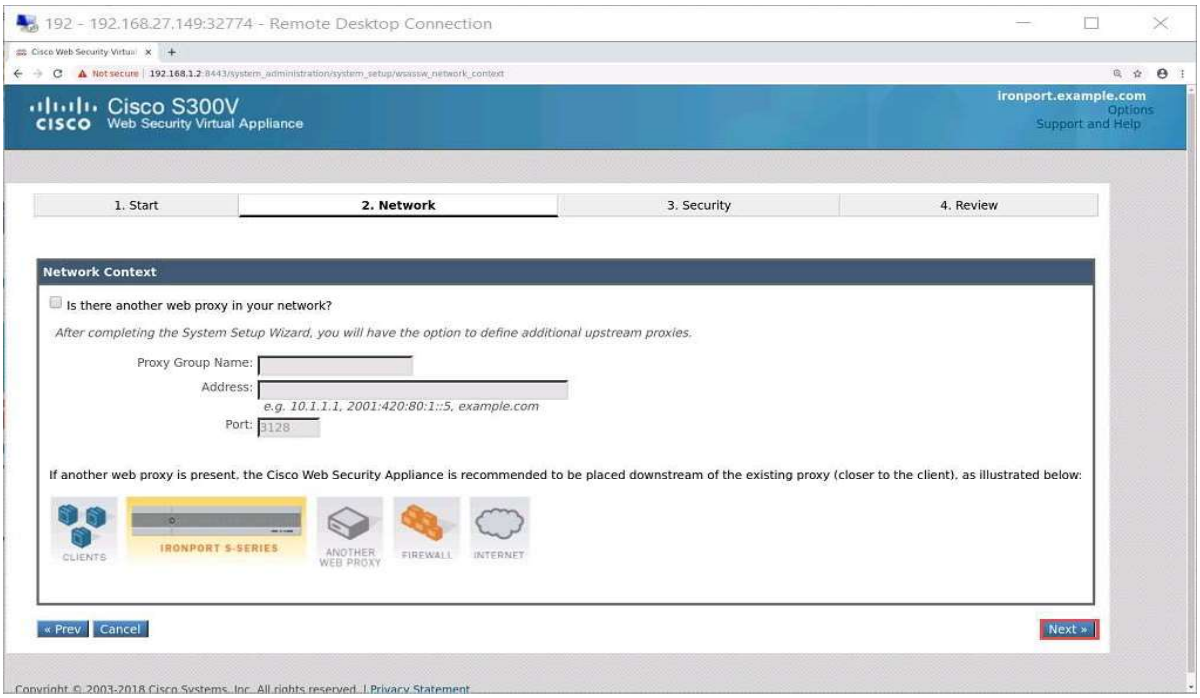
3. **Setup System Wizard**

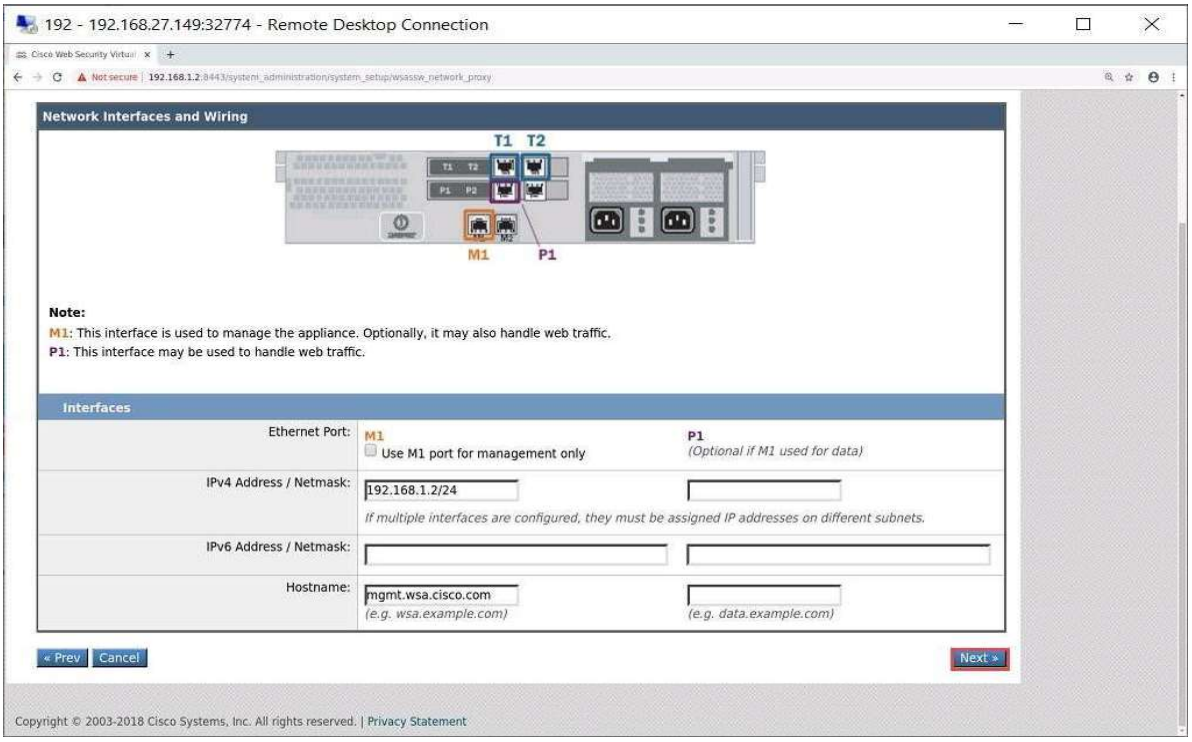
   ***** First add ip to MGMT windows PC 192.168.1.1 *****

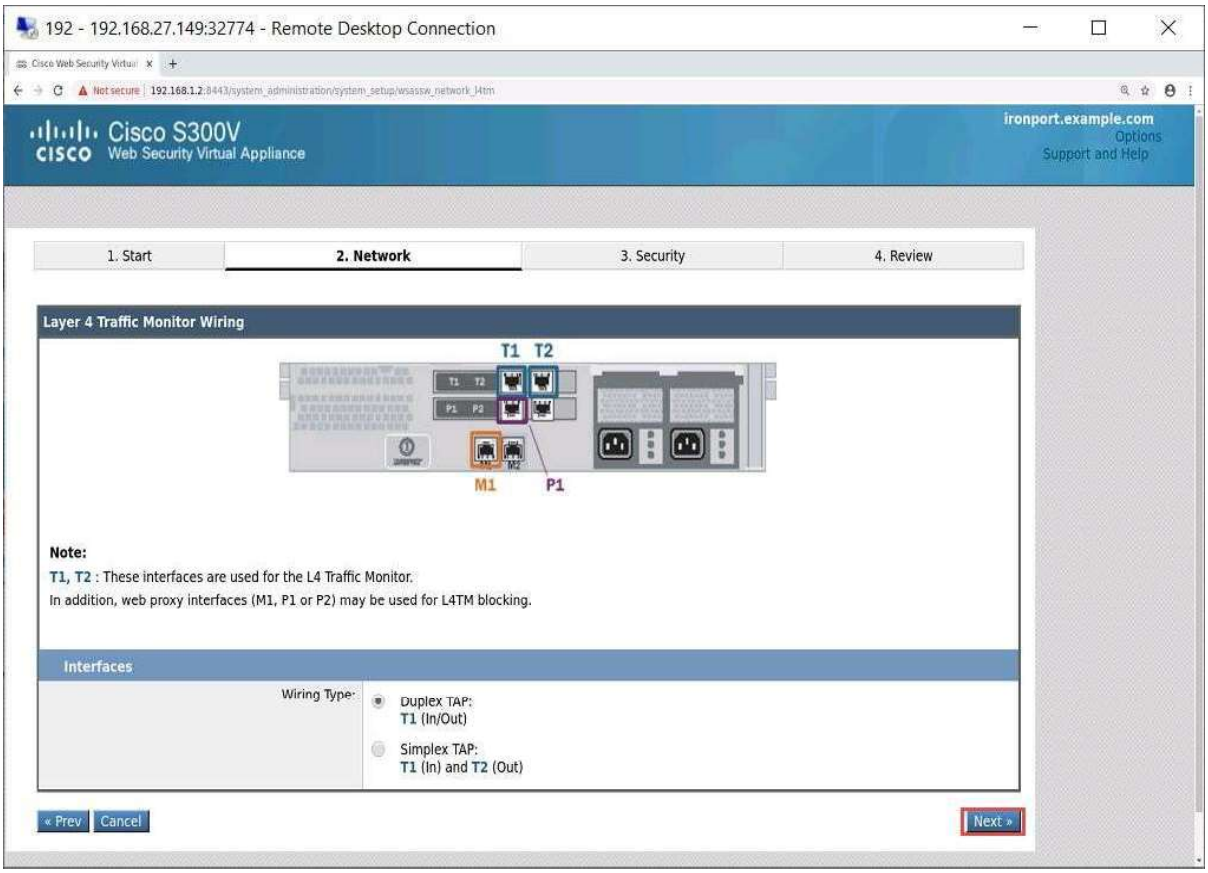
Click MGMT PC and http://192.168.1.2

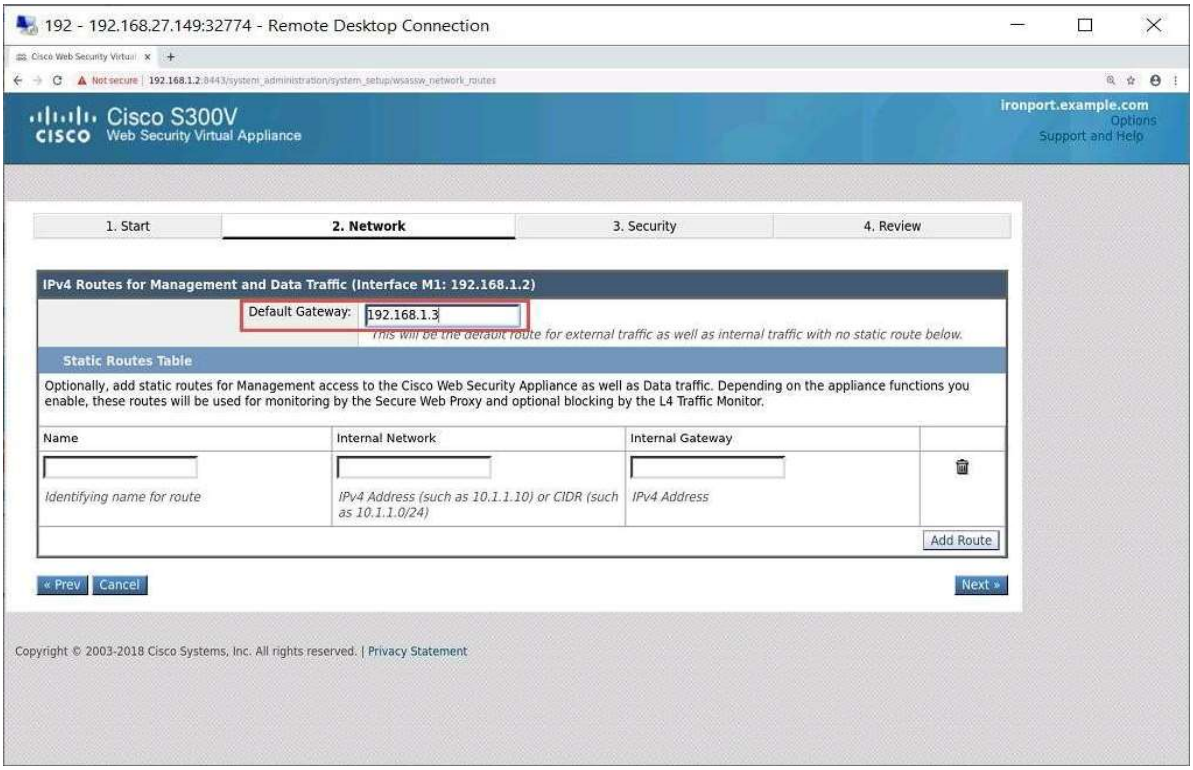

192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco S300V
Web Security Virtual Appliance
Logged in as: admin on ironport.example.com
My Favorites
Options
Support and Help
Reporting
Web Security Manager
Security Services
Network
System Administration
No Changes Pending
Transparent Redirection
Transparent Redirection Device
The Web Proxy is not configured. To change basic deployment options, please run the System Setup W
System Setup Wizard).
Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement
Policy Trace
Alerts
Log Subscriptions
Return Addresses
SSL Configuration
Users
Network Access
System Time
Time Zone
Time Settings
Configuration
Configuration Summary
Configuration File
Feature Key Settings
Feature Keys
Upgrade and Updates
Upgrade and Update Settings
System Upgrade
System Setup
System Setup Wizard

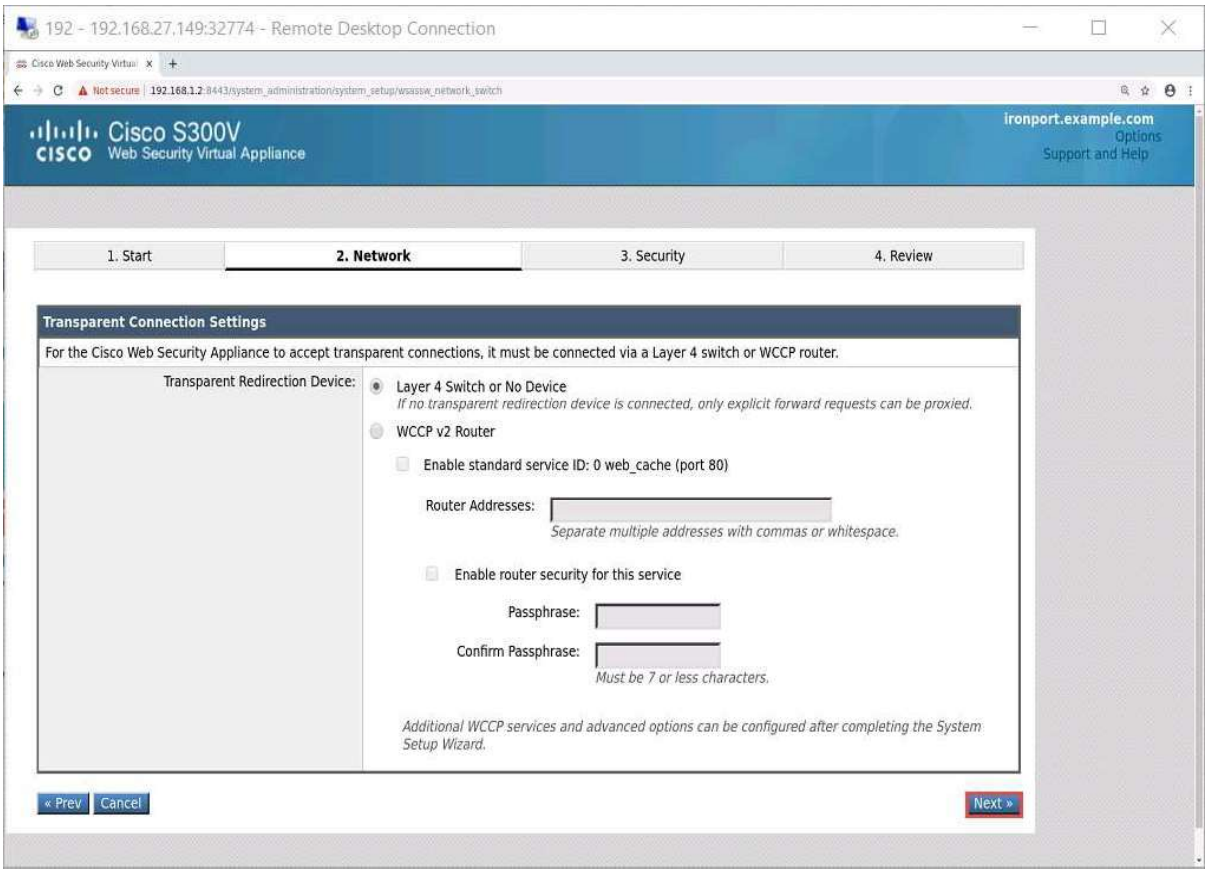

192 - 192.168.27.149:32774 - Remote Desktop Connection
1. Start
2. Network
3. Security
4. Review
System Settings
Default System Hostname:
wsa.cisco.com
e.g. proxy.company.com
DNS Server(s):
Use the Internet's Root DNS Servers
Use these DNS Servers:
(optional)
(optional)
NTP Server:
time.sco.cisco.com
Time Zone:
Region:
GMT Offset
Country:
GMT
Time Zone / GMT Offset:
GMT
Appliance Mode
Appliance Mode of Operation
Standard
This appliance will be used for on-premise policy enforcement (Standard Web Security Appliance installation).
Cloud Web Security Connector
This appliance will be used primarily to direct traffic to Cisco Cloud Web Security for cloud policy enforcement and threat defense (Cloud Web Security Connector installation).
« Prev
Cancel
Next »

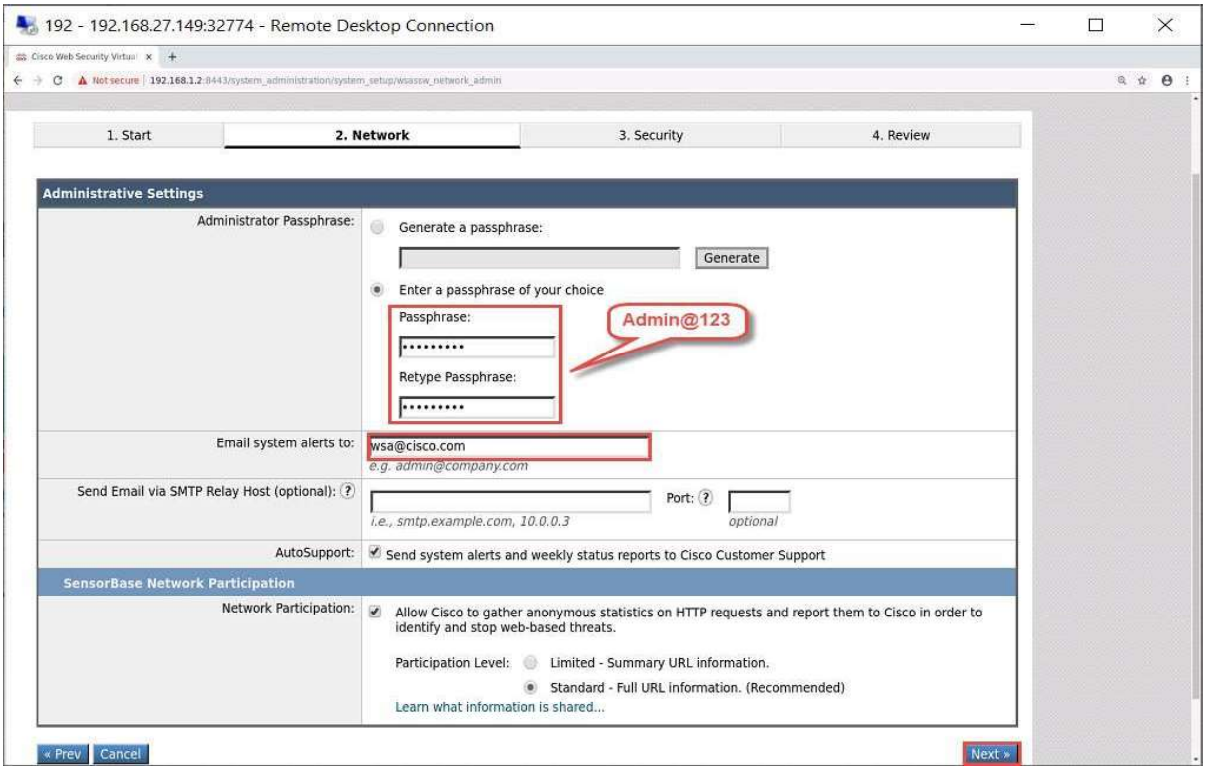

192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco S300V
Web Security Virtual Appliance
ironport.example.com
Options
Support and Help
1. Start
2. Network
3. Security
4. Review
Network Context
Is there another web proxy in your network?
After completing the System Setup Wizard, you will have the option to define additional upstream proxies.
Proxy Group Name:
Address:
e.g. 10.1.1.1, 2001:420:80:1::5, example.com
Port:
3128
If another web proxy is present, the Cisco Web Security Appliance is recommended to be placed downstream of the existing proxy (closer to the client), as illustrated below:
CLIENTS
IRONPORT S-SERIES
ANOTHER WEB PROXY
FIREWALL
INTERNET
« Prev
Cancel
Next »
Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement

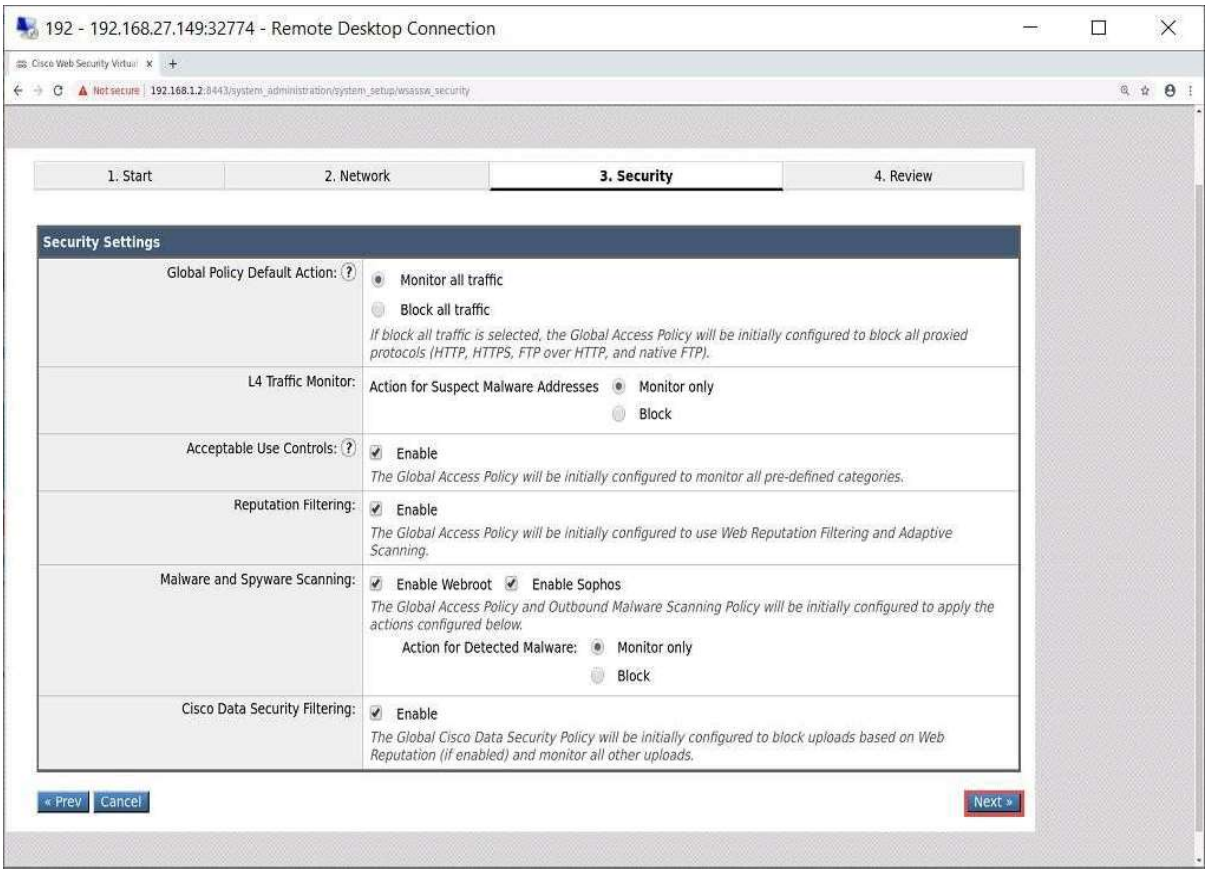

192 - 192.168.27.149:32774 - Remote Desktop Connection
Network Interfaces and Wiring
T1 T2
M1
P1
Note:
M1: This interface is used to manage the appliance. Optionally, it may also handle web traffic.
P1: This interface may be used to handle web traffic.
Interfaces
Ethernet Port:
M1
Use M1 port for management only
P1
(Optional if M1 used for data)
IPv4 Address / Netmask:
192.168.1.2/24
If multiple interfaces are configured, they must be assigned IP addresses on different subnets.
IPv6 Address / Netmask:
Hostname:
mgmt.wsa.cisco.com
(e.g. wsa.example.com)
(e.g. data.example.com)
« Prev
Cancel
Next »
Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement


192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco S300V
Web Security Virtual Appliance
ironport.example.com
Options
Support and Help
1. Start
2. Network
3. Security
4. Review
Layer 4 Traffic Monitor Wiring
T1 T2
M1
P1
Note:
T1, T2 : These interfaces are used for the L4 Traffic Monitor.
In addition, web proxy interfaces (M1, P1 or P2) may be used for L4TM blocking.
Interfaces
Wiring Type:
Duplex TAP:
T1 (In/Out)
Simplex TAP:
T1 (In) and T2 (Out)
« Prev
Cancel
Next »


192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco S300V
Web Security Virtual Appliance
ironport.example.com
Options
Support and Help
1. Start
2. Network
3. Security
4. Review
IPv4 Routes for Management and Data Traffic (Interface M1: 192.168.1.2)
Default Gateway:
192.168.1.3
This will be the default route for external traffic as well as internal traffic with no static route below.
Static Routes Table
Optionally, add static routes for Management access to the Cisco Web Security Appliance as well as Data traffic. Depending on the appliance functions you enable, these routes will be used for monitoring by the Secure Web Proxy and optional blocking by the L4 Traffic Monitor.
Name
Internal Network
Internal Gateway
Identifying name for route
IPv4 Address (such as 10.1.1.10) or CIDR (such as 10.1.1.0/24)
IPv4 Address
Add Route
« Prev
Cancel
Next »
Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | Privacy Statement


192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco S300V
Web Security Virtual Appliance
ironport.example.com
Options
Support and Help
1. Start
2. Network
3. Security
4. Review
Transparent Connection Settings
For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.
Transparent Redirection Device:
Layer 4 Switch or No Device
If no transparent redirection device is connected, only explicit forward requests can be proxied.
WCCP v2 Router
Enable standard service ID: 0 web_cache (port 80)
Router Addresses:
Separate multiple addresses with commas or whitespace.
Enable router security for this service
Passphrase:
Confirm Passphrase:
Must be 7 or less characters.
Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.
« Prev
Cancel
Next »


192 - 192.168.27.149:32774 - Remote Desktop Connection
1. Start
2. Network
3. Security
4. Review
Administrative Settings
Administrator Passphrase:
Generate a passphrase:
Generate
Enter a passphrase of your choice
Passphrase:
Retype Passphrase:
Admin@123
Email system alerts to:
wsa@cisco.com
e.g. admin@company.com
Send Email via SMTP Relay Host (optional):
Port:
i.e., smtp.example.com, 10.0.0.3
optional
AutoSupport:
Send system alerts and weekly status reports to Cisco Customer Support
SensorBase Network Participation
Network Participation:
Allow Cisco to gather anonymous statistics on HTTP requests and report them to Cisco in order to identify and stop web-based threats.
Participation Level:
Limited - Summary URL information.
Standard - Full URL information. (Recommended)
Learn what information is shared...
« Prev
Cancel
Next »


192 - 192.168.27.149:32774 - Remote Desktop Connection
Cisco Web Security Virtual
Not secure | 192.168.1.2:8443/system_administration/system_setup/wsassa_security
1. Start
2. Network
3. Security
4. Review
Security Settings
Global Policy Default Action:
Monitor all traffic
Block all traffic
If block all traffic is selected, the Global Access Policy will be initially configured to block all proxied protocols (HTTP, HTTPS, FTP over HTTP, and native FTP).
L4 Traffic Monitor:
Action for Suspect Malware Addresses
Monitor only
Block
Acceptable Use Controls:
Enable
The Global Access Policy will be initially configured to monitor all pre-defined categories.
Reputation Filtering:
Enable
The Global Access Policy will be initially configured to use Web Reputation Filtering and Adaptive Scanning.
Malware and Spyware Scanning:
Enable Webroot
Enable Sophos
The Global Access Policy and Outbound Malware Scanning Policy will be initially configured to apply the actions configured below.
Action for Detected Malware:
Monitor only
Block
Cisco Data Security Filtering:
Enable
The Global Cisco Data Security Policy will be initially configured to block uploads based on Web Reputation (if enabled) and monitor all other uploads.
« Prev
Cancel
Next »