CISCO CERTIFIED

CCNP

SECURITY

SCOR 350-701

08- Web Content Security (WSA)

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Cisco WSA Overview

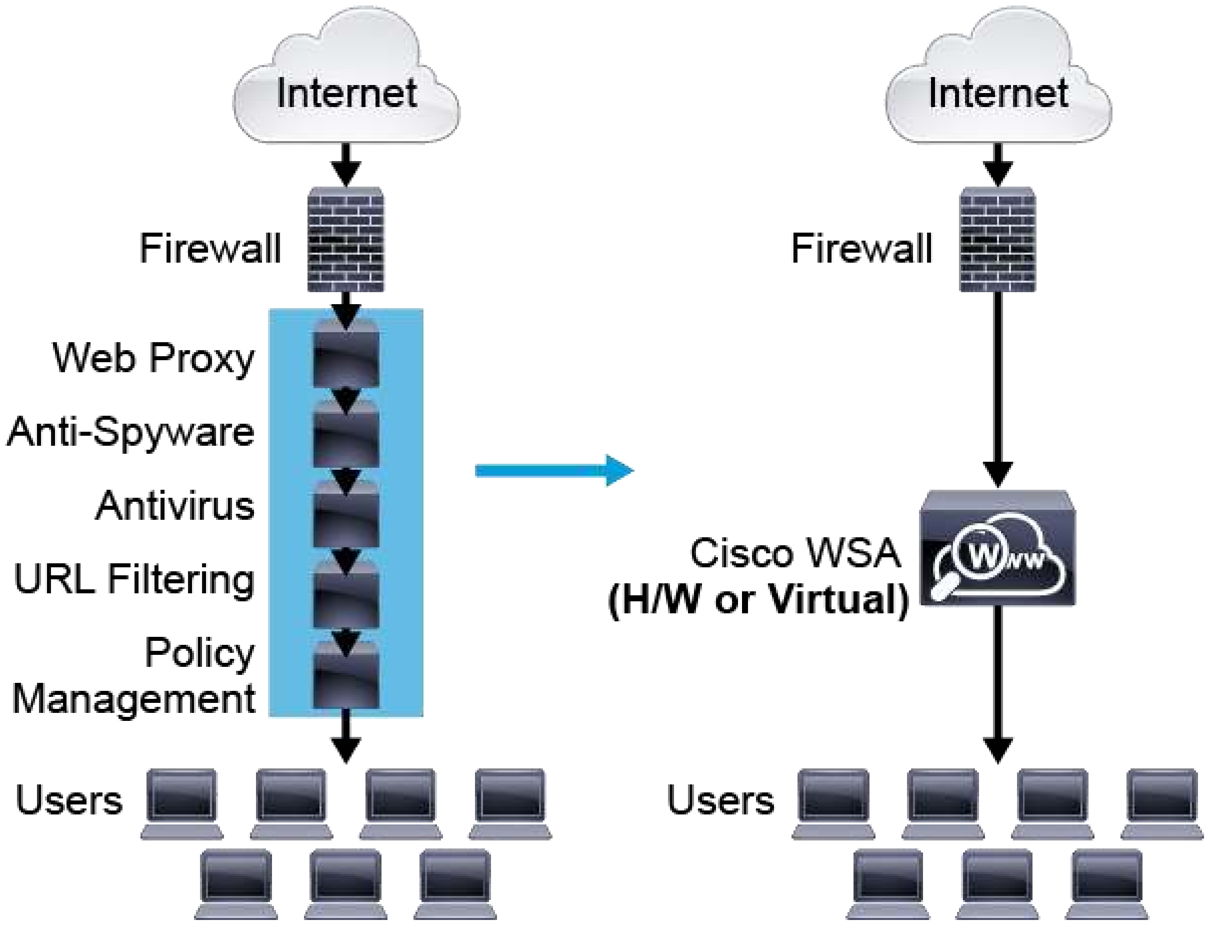
- Web access is a requirement for the day-to-day functions of most organizations.
- The challenge is maintaining appropriate web access for everyone in the organization while minimizing unacceptable or risky use.
- A solution is needed to control policy-based web access to ensure employees work effectively and confirm that personal web activity does not waste bandwidth, affect productivity, or expose the organization to undue risk.
- One risk that is associated with internet access for organizations is the pervasive threat that exists from accessing websites that contain malicious and harmful content.
- Therefore, organizations must have an appropriate protection against everyday threats such as viruses, Trojans, worms, or botnet attacks that might be initiated by the employees.

Cisco WSA Overview (cont.)

- The Cisco WSA solution complements the deep packet inspection and stateful filtering capabilities of the firewalls by providing additional web security features using a dedicated on-premises appliance.

- A key characteristic of the Cisco WSA is that web proxy, antispyware, antivirus, URL filtering and policy management among many other things are all managed on the same appliance (that can be deployed as a hardware or as a virtual appliance), instead of running on separate appliances.

Cisco WSA Overview (cont.)



Cisco WSA Overview (cont.)

Cisco WSA deployment enables four main security capabilities:

1. **Transparent redirection of user web traffic:** Through the seamless integration with the Cisco ASA Firewall or Cisco Firepower Next-Generation Firewall (NGFW), web traffic is transparently redirected to Cisco WSA service. No configuration changes are required on user devices and all traffic is inspected by the Cisco WSA, before web access is provided to users.

2. **Web filtering:** Cisco WSA supports URL filters that are based on predefined content categories and custom categories. Filtering rules can be configured to block, monitor, or warn, based on the specific web usage policies of an organization. This easily allows organizations to block access to websites that belong specific URL category.

Cisco WSA Overview (cont.)

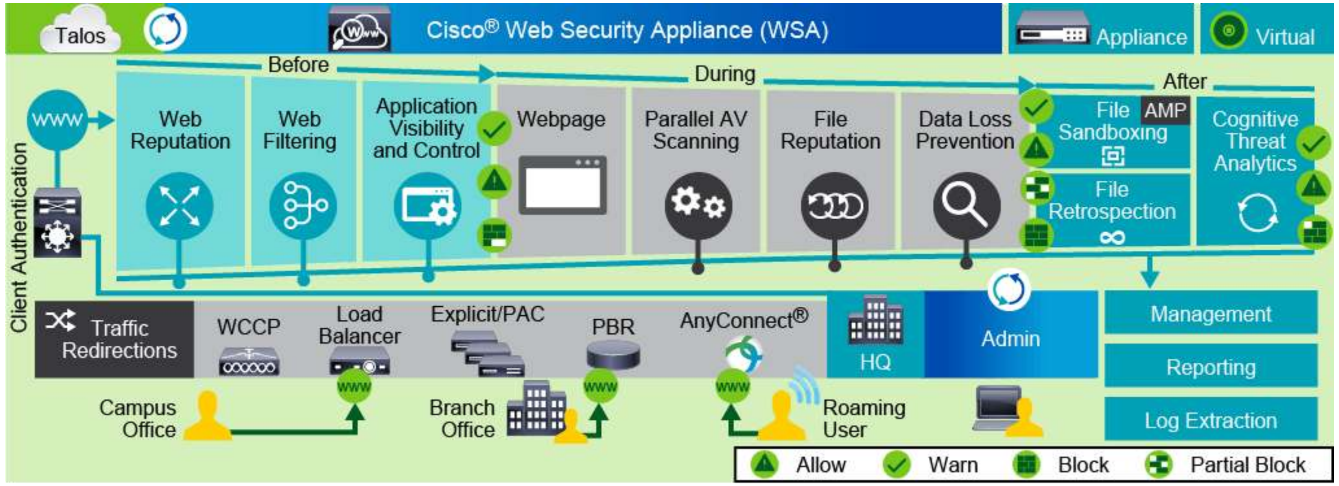
Cisco WSA deployment enables four main security capabilities (cont.)

3. **Malware protection:** Cisco WSA analyzes every web request to determine if content is malicious. Using Dynamic Vectoring and Streaming (DVS) engine with **Webroot**, **McAfee**, and **Sophos** anti-malware scanning engines, helps organizations secure business applications and processes through identification, prevention, and remediation of threats. Also, the Cisco AMP as an add-on licensed feature provides malware detection and blocking, continuous analysis, and retrospective alerting.

4. **Differentiated policies:** Policies for Cisco WSA are applied on a per-group basis. Identity determines group membership and can include authenticated user information or the source IP address of the web request. This allows different actions to be performed on different groups of users.

Cisco WSA Overview (cont.)

- Cisco WSA safeguards businesses through broad-threat intelligence, multiple layers of malware defense, and vital DLP capabilities across the attack continuum.
- The whole process is divided into three separate segments of protection:
  1. Before an attack occurs
  2. During an attack
  3. After an attack occurs



Cisco WSA Overview (cont.)

- The Cisco WSA appliance detects and correlates threats in real time by tapping into the largest threat-detection network in the world, **Cisco Talos**.
- To discover where threats are hiding, **Cisco Talos** pulls massive quantities of information across multiple vectors such as a firewall, intrusion prevention system (IPS), web, email, and VPN.
- **Cisco Talos continuously refreshes information every 3 to 5 minutes**, adding and receiving intelligence from Cisco WSA and other network security devices.
- This first protection step consists of using web reputation filters and Cisco web usage controls (Application Visibility and Control [AVC]).

Cisco WSA Overview (cont.)

Design Overview

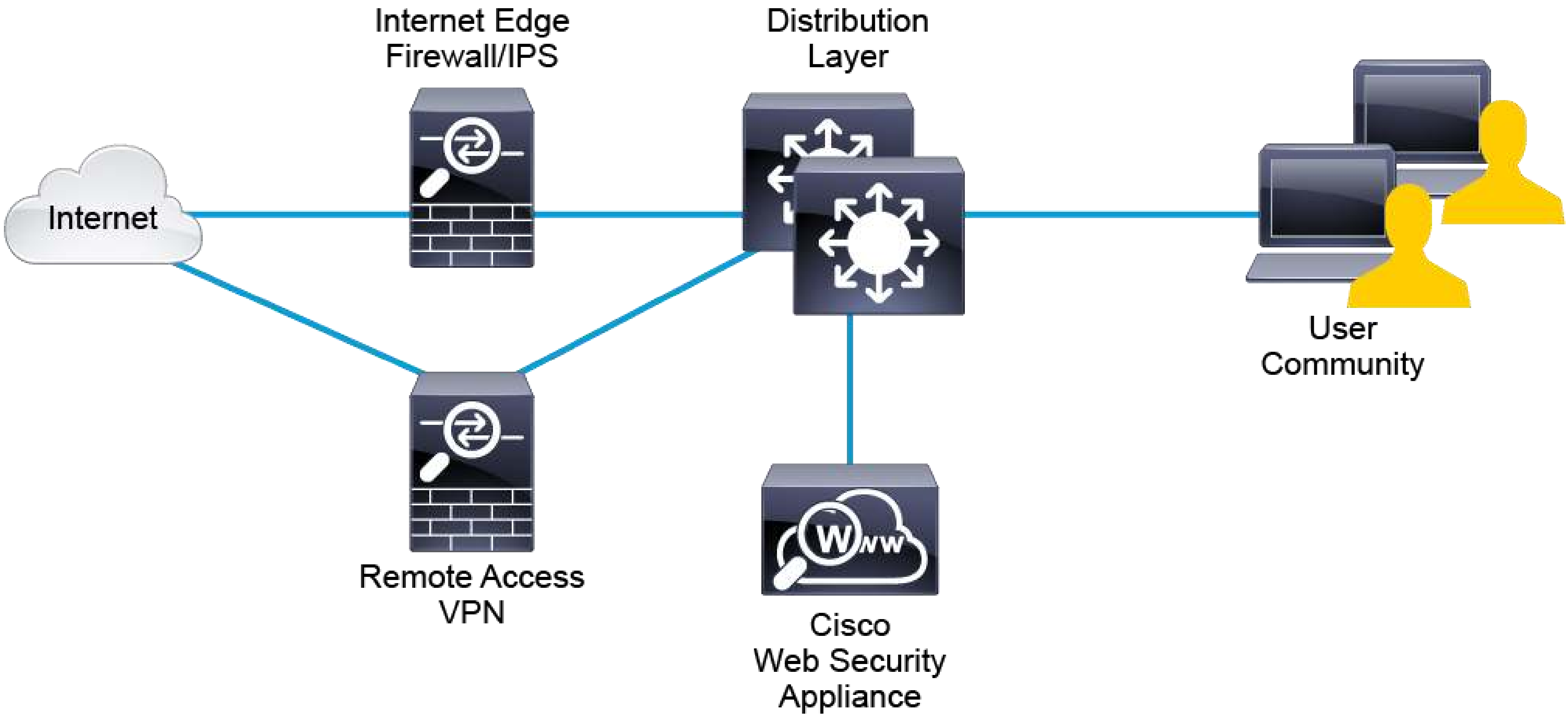
- Using only a Cisco ASA Firewall or a Cisco Firepower NGFW in a corporate network provides significant protection against malicious web traffic, but there are some limitations in this approach for achieving full web protection.
- Therefore, there is a requirement for implementation of a more advanced filtering technique and features that are capable of performing more detailed inspections and traffic filtering actions based on the organization requirements.
- **Cisco WSA** addresses the need for a corporate web security policy by offering a combination of web usage controls with **category** and **reputation-based control**, **malware filtering**, and **data protection**.

Cisco WSA Overview (cont.)

Design Overview (cont.)

- Browsing websites can be risky since websites inadvertently end up distributing compromised or malicious content as a result of inattention to update requirements or lax security configurations.
- Websites that serve the compromised and malicious content are constantly changing as human-operated and worm-infested computers scan the internet in search of additional web servers that they can infect to continue propagating.
- This dynamic environment introduces significant challenges to maintain up-to-date Internet threat profiles.

Cisco WSA Overview (cont.)



Cisco WSA Overview (cont.)

- All these potential threats that can be harmful to the assets of the organization and could be easily denied by implementing and properly configuring a Cisco WSA appliance in the environment*.*
- The Cisco WSA solution protects against malicious web traffic initiated from the outside and from the inside the network*.*
- When remote users access websites over the internet, additional protection can be provided to all VPN traffic by Cisco WSA inspection.
- This protection can be accomplished by implementing policies on network devices, such as **Cisco ASA firewall** or **Cisco Firepower NGFW**, for <u>redirecting web traffic to the Cisco WSA</u> for performing advanced filtering against malicious HTTP, HTTPS, or FTP traffic.

Cisco WSA Overview (cont.)

- Several features of the Cisco WSA (such as AVC, URL filtering and AMP) are also integrated in the Cisco Firepower NGFW.
- The Cisco Firepower NGFW solution is implemented inline in the networks, whereas the Cisco WSA operates as **an explicit web proxy**.
- Once the web traffic is received on the Cisco Firepower NGFW, it is filtered out inline, and no additional steps are involved.
- When the Cisco WSA operates in the **transparent proxy mode**, it requires redirection of the web traffic from other network devices to itself where it is processed and then allowed or denied based on the local policies.

Cisco WSA Overview (cont.)

- Although there is some **overlap** in features between the Cisco WSA and the inline Cisco Firepower NGFW, **it is recommended** to use Cisco WSA for pure filtering of only web traffic going in and out in the network.
- One of the reasons for that is because the Cisco WSA operates as a standalone appliance (hardware or virtual) just for filtering web traffic (and not other data that passes through the network), which makes the overall management of web traffic easier.
- Moreover, it provides additional features, (such as better HTTPS decryption capabilities, rate limiting, caching, better reporting) that are unique in their own way and are implemented on a more advance level in the Cisco WSA.

Cisco WSA Overview (cont.)

There are two methods can be used for sending web traffic to the **Cisco WSA**

1. Transparent proxy mode

   ✓ The user is unaware of using a web proxy, Once the traffic is sent, an extra network device redirects the web traffic to the Cisco WSA for filtering.

2. Explicit proxy mode

   ✓ The user is aware of having a web proxy in the network so all web traffic is directly sent to the Cisco WSA.

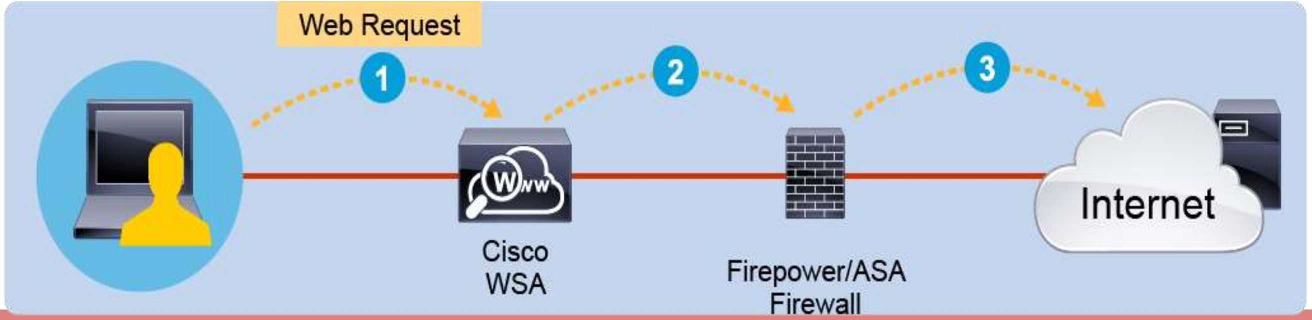
Cisco WSA Depoymnt Options (cont.)

Deployment	Method	Description
Transparent	WCCP	A WCCP enabled device such as router, switch, or firewall redirects port 80 (and possibly port 443) traffic
Explicit forward	Browser configured	Client browser is explicitly configured to use a proxy; hence all web traffic is sent to the Cisco WSA
Explicit forward	.PAC file that is configured	Client browser is explicitly configured to use a .PAC file, which in turn, references the proxy (Cisco WSA)

Cisco WSA Depoymnt Options (cont.)

1- Explicit Deployment Mode

- In explicit forward mode, the user intentionally connects to a web proxy.
- For every website that a user tries to open, a web request is sent to the Cisco WSA.
- Because of this direct communication between the user and the web proxy, there is no need for additional network device to intercept and redirect the web traffic to the Cisco WSA.
- Once the web traffic is received by the Cisco WSA, it resolves the server name in the URL and communicates with the remote web server on behalf of the user.



Cisco WSA Depoymnt Options (cont.)

In explicit proxy deployment, several steps are performed when the internal user initiates a web session to the web server:

1. An internal user makes a web request to an external web server, Because the client browser is configured to use a web proxy, it sends the request directly to the Cisco WSA.
2. The Cisco WSA connects to the web server on behalf of the internal user.
3. The firewall (Cisco Firepower NGFW or Cisco ASA) is configured to allow only outbound web traffic coming from the Cisco WSA, and forwards it to the destination web server.

Cisco WSA Depoymnt Options (cont.)

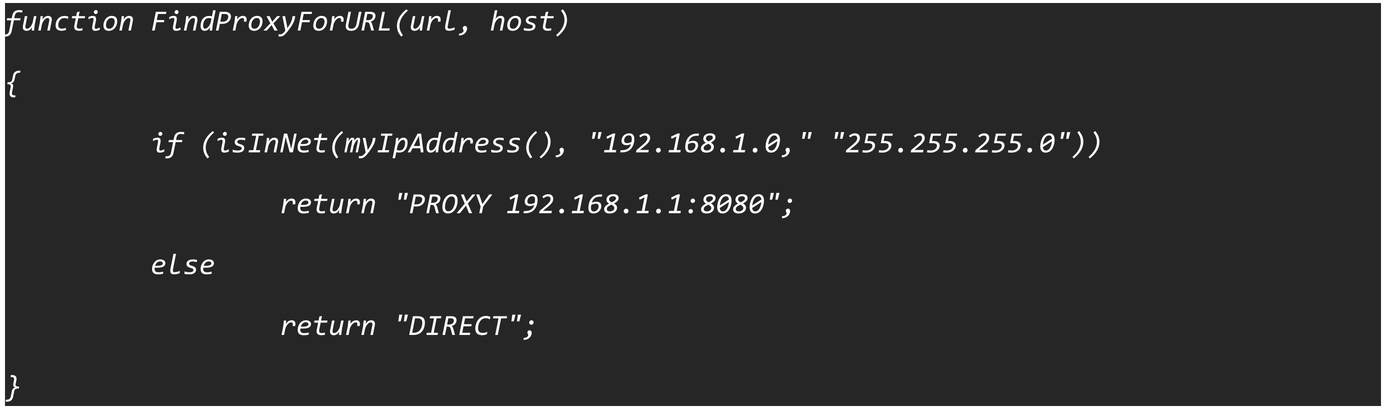
PAC Files

- PAC files can be used to deploy explicit forward proxy uniformly on many clients.
- A PAC file is a language to inform web browsers how to use proxies on their networks.
- PAC files allow you to configure a compliant browser to access web-based resources, either directly or through a proxy server.
- The use of PAC files avoids any configuration on the user's end devices.
- Some of the most important features that PAC files support are load balancing and failover.

Cisco WSA Depoymnt Options (cont.)

PAC Files (cont.)

- The PAC file checks the local IP subnet address of the PC and then decides based on IF/ELSE statements.
- If the PC is located in a subnet that matches, a proxy server is used, If the PC is on any other subnet, a direct connection is used instead of the proxy.



```
function FindProxyForURL(url, host)
{
        if (isInNet(myIpAddress(), "192.168.1.0," "255.255.255.0"))
                return "PROXY 192.168.1.1:8080";
        else
                return "DIRECT";
}
```

Cisco WSA Depoymnt Options (cont.)

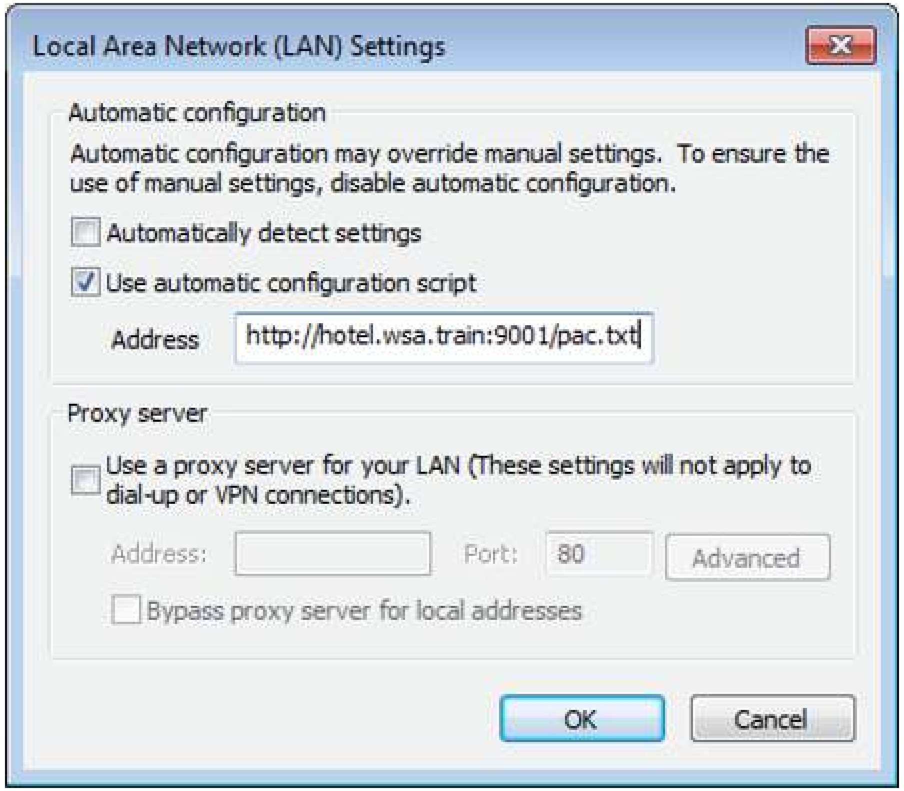
PAC Files (cont.)

- The PAC files can be hosted in these three locations:

1. **Web servers:** The web server should be configured to serve a PAC.
2. **Cisco WSA:** You can place PAC files on a Cisco WSA, which appears to clients as a web browser.
3. **Local machines:** You can place the PAC file locally on a user's hard disk.

Cisco WSA Depoymnt Options (cont.)

PAC Files (cont.)



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☑ Use automatic configuration script

Address: http://hotel.wsa.train:9001/pac.txt

Proxy server

☐ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

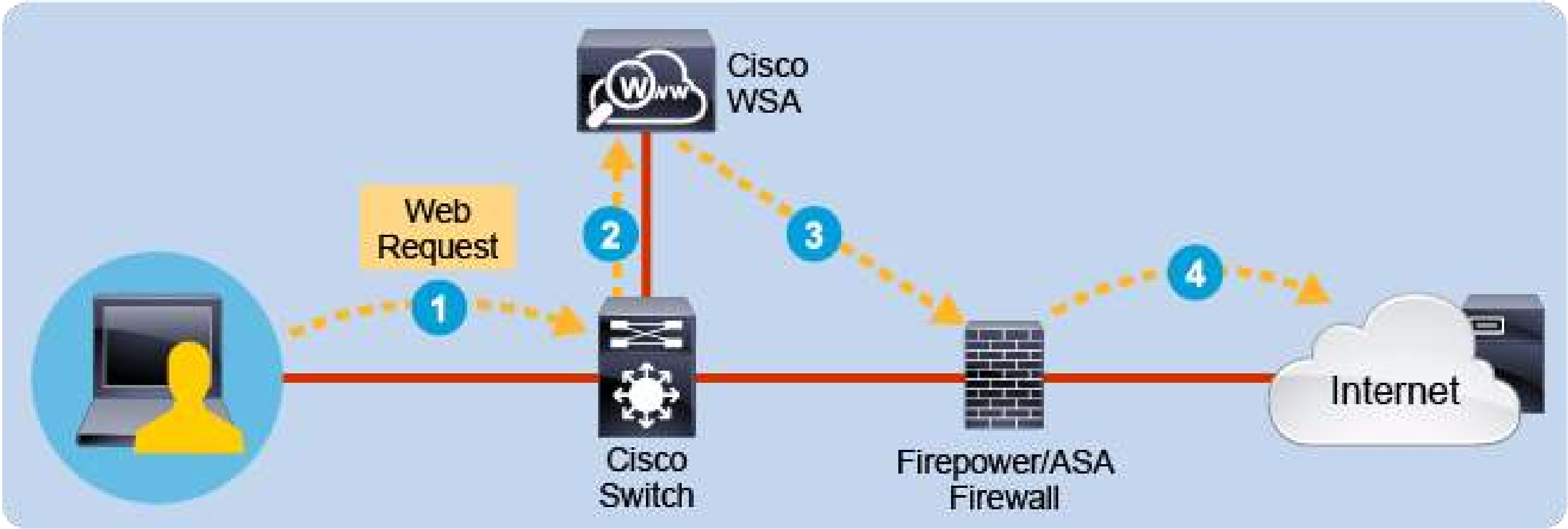
☐ Bypass proxy server for local addresses

Cisco WSA Depoymnt Options (cont.)

2- Transparent Deployment Mode

- In transparent proxy mode, the user is unaware of a web proxy being used in the network.
- When the user tries to open a website, the web request is directed to the target web server, instead of the web proxy.
- In transparent proxy mode, the client resolves the hostname of the target web server.
- A network device such as Cisco switch, router, or firewall intercepts the web request and redirects it to the Cisco WSA.
- This redirection can be implemented on various network devices that support the **Web Cache Communication Protocol** (**WCCP**) protocol or policy-based routing (**PBR**).

Cisco WSA Depoymnt Options (cont.)



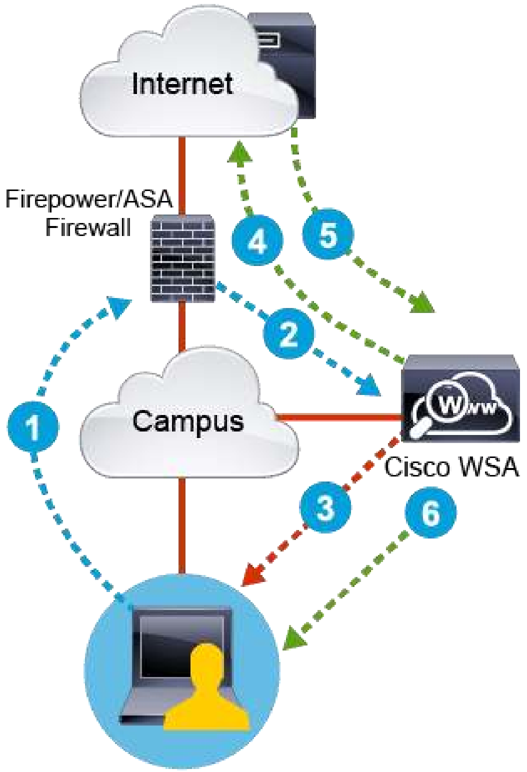
Cisco WSA Depoymnt Options (cont.)

Web Cache Control Protocol

- The WCCP is a content-routing technology developed by Cisco that intercepts IP packets and redirects them to a different destination than the one that is specified in the IP packet.
- WCCP is available on many network devices, including the following:
  1. Cisco ASA firewall
  2. Cisco Firepower NGFW
  3. Cisco Aggregation Service Routers (ASR) router
  4. Cisco Catalyst switches

Cisco WSA Depoymnt Options (cont.)

Web Cache Control Protocol (cont.)



Cisco WSA Depoymnt Options (cont.)

Web Cache Control Protocol (cont.)

The WCCP process is as follows:

1. The user initiates a web request.
2. The Cisco ASA Firewall redirects the request to the Cisco WSA by using WCCP.
3. The Cisco WSA checks the request and replies with a denial if the request violates policy.
4. The Cisco WSA initiates a new connection to the web if the request is acceptable.
5. The Web server replies with content, which is sent to the Cisco WSA.
6. The Cisco WSA checks content for objectionable material and forwards content to the originating user if no issues are encountered.