**Cisco WSA overview**

* 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
* The Cisco WSA is a web proxy that works with other Cisco network components (such as firewalls, routers, or switches) to monitor and control web content requests from within the organization. It also inspects the return web traffic for any malicious content
* Cisco WSA offers four main security capabilities
  + **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. All traffic is inspected by the Cisco WSA, before web access is provided to users.
  + **Web filtering:** Filtering rules can be configured to block, monitor, or warn, based on the specific web usage policies of an organization.
  + **Malware protection**: Cisco WSA analyzes every web request to determine if content is malicious.
  + **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.

The Cisco WSA solution offers these additional capabilities for web traffic protection:

* + **Single appliance security and control:**
  + **Advanced threat defense:** The Cisco WSA protects against both, known and emerging potential threats to the enterprises, by using advanced security features provided by the Cisco Talos Security Intelligence and Research Group (Talos).
  + **Granular acceptable use policy:** Enterprises can increase the amount of time that employees spend on business-oriented activities, reducing misuse of enterprise networks and bandwidth.
  + **Centralized management and reporting:** The Cisco WSA provides an easy-to-use, centralized management tool to control operations, manage policies, and view reports. The Cisco Security Management Appliance (SMA) provides central management and reporting across multiple Cisco Web Security Appliances (WSAs).
  + **Deep web usage and application visibility:**
  + **Roaming-User Protection:** The Cisco WSA protects roaming users by integrating with the Cisco AnyConnect Secure Mobility Client, which provides web security to remote clients by initiating a VPN tunnel that redirects traffic back to the on-premises solution.
  + **Flexible Deployment:** The Cisco Web Security Virtual Appliance (WSAV) offers all the same features as the Cisco WSA, with the added convenience and cost savings of a virtual deployment model, including instant self-service provisioning
  + **Data loss prevention:** The Cisco WSA blocks sensitive information from leaving the safety of the network, helping to ensure compliance and reduce risk.

**Design overview**

* Two methods that can be used for sending web traffic to the Cisco WSA: ***transparent proxy mode* and *explicit proxy mode*.**
* **Explicit mode**: the user is aware(conscient) of having a web proxy in the network so all web traffic is directly sent to the Cisco WSA.
* In **transparent 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.

**Logical traffic flow using cisco WSA consists of the following steps:**

* User initiates web request, which is redirected to WSA (explicity or transparently)
* The cisco WSA checks the request and if does not violate policy, forwards it to the web server
* Web server replies with content which is sent to cisco WSA
* Cisco wsa checks content for objectionable materials and forwards it to the user if no issues are found

**Cisco WSA Features**

The Cisco WSA runs on the Cisco proprietary AsyncOS that includes **three software blades**, **management and reporting tools, and a custom operating system platform.** The term *blade* is used to create an analogy with physical blades. **These blades (Acceptable User Policy, Malware Defense, and Data Security)** are software components that are installed on every Cisco WSA product and consist of many different security features that are optionally enabled by licenses.



**Management and reporting capabilities**

* Web security manager: **:** Cisco web security manager provides a single and easy-to-understand view of all access and security policies that are configured on the appliance
* Web security monitor: Cisco web security monitor offers a valuable insight into overall web activity, and threat identification and prevention, within corporate networks.
* Logging: Extensive logging allows enterprises to track all web traffic, benign, and malware related
* Integrated authentication
* Multiple deployment modes

**Acceptable use policy enforcement**

* Web proxy: It allows for deep content analysis, which is critical to accurately detect devious and rapidly mutating web-based malware
* URL Filters
* **Acceptable use policy, application, and protocol control:** Acceptable use policy (AUP), application, and protocol control are facilitated at a granular level, regardless of the protocol or application flowing through the network perimeter

**Malware defense features**

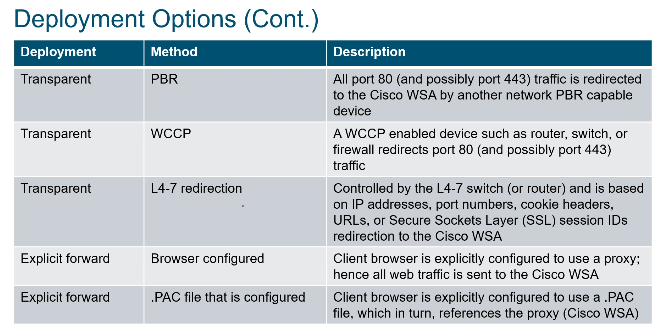
* Layer 4 traffic monitor
* Cisco security intelligence operations
* Web reputation filters
* Antimalware system
* Scanning engine
* DVS engine
* HTTPS decryption

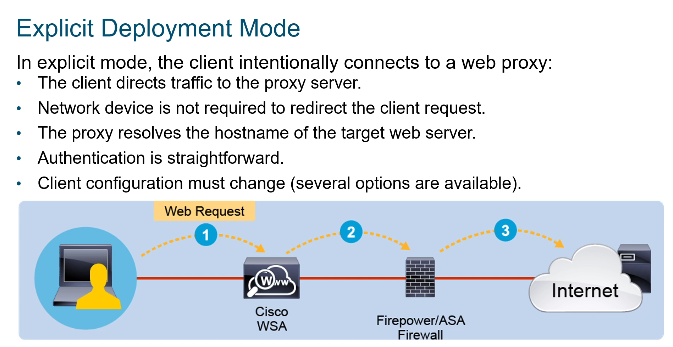
**Data security enforcement:**

* Data lost prevention
* Native FTP protection: Native FTP protection allows Cisco WSA to provide complete visibility into FTP usage, enforcing acceptable use and data security policies, and preventing malware infections

**Deployments options**

The cisco WSA can operate as a web proxy that actively inspect web traffic or as a Layer 4 traffic Monitor (L4TM) that passively inspects web traffic





**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.
* 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*.**
* There are two options that can help the user to find the PAC file and use the settings to connect to the web proxy:
  + Configure the users with the PAC file location, by specifying a URL that specifically points to the PAC file.
  + Configure the users to locate the PAC files automatically using the Web Proxy Auto-Discovery (WPAD) protocol along with DHCP or DNS.
* PAC files can be hosted in web severs, cisco wsa, local machines

**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.

Transparent mode traffic redirection

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
* available on many switches, routers, and firewalls
* No configuration required on user side
* Built features: load balancing, scaling, fault tolerance

PBR: Forwarding and routing data packets based on policies, instead of destination network

Layer 4-7 switch: redirect traffic based on IP addresses, port numbers, cookie headers, URL or SSL session ID, support load balancing and failover. Provides passive protection against suspicious TCP /UDP sessions

**FTP Proxy and SOCKS Proxy Overview**

The web proxy can intercept web requests that use the HTTP (including FTP over HTTP) and HTTPS protocols. In addition to this, the Cisco WSA supports two other proxy types that can help to enhance the protocol management:

* **FTP proxy:** The FTP Proxy allows the interception of native FTP traffic communication between the user and the server, rather than just FTP traffic that has been encoded within the HTTP protocol.
* **SOCKS proxy:** The SOCKS proxy allows the interception of SOCKS traffic initiated from the user and destined to the application server.

Cisco WSA High Availability Overview

With explicit deployments, high-availability functionality could be achieved using different approaches:

* **Load balancer:** Using a dedicated load balancer that would load balance the web traffic across different Cisco WSAs.
* PAC file: PAC files contain entries directing clients to multiple Cisco WSAs based on various network factors or machine characteristics.
* **Common Address Redundancy Protocol:** The CARP protocol provides a high-availability functionality. This protocol is built into the AsyncOS operating system and uses the virtual IP address approach.

**Network Users Authentication**

The Cisco WSA can authenticate users before Internet access is provided:

* Requirements for authentication:
  1. Provide different policies to different users and groups of users
  2. Track employee use of the internet
* Cisco WSA Authentication:
  1. Tracks and reports on users by username instead of IP address
  2. Integrates with existing authentication infrastructure
  3. Used as a prerequisite for enforcing distinct policies for different users and groups:
     + Identity, role or group assignment
     + Allowance for specific user agents (browsers)
     + Restriction of certain protocols, and so on

**Cisco WSA Authentication overview**

Cisco WSA supports different authentication types

* **Active authentication**: the Cisco WSA prompts the user for credentials, which afterwards checks them against an external server that can be an Active Directory or LDAP server.
* **Passive authentication**: the Cisco WSA is integrated with an external source such as Cisco Context Directory Agent (CDA) or Cisco ISE. These external sources provide transparent authentication because the users are not prompted for any credentials, but they are provided by the Cisco CDA or Cisco ISE
* Active directory supports three authentication schemes: Kerberos, NTLMSSP, Basic
* LDAP supports only the basic authentication scheme

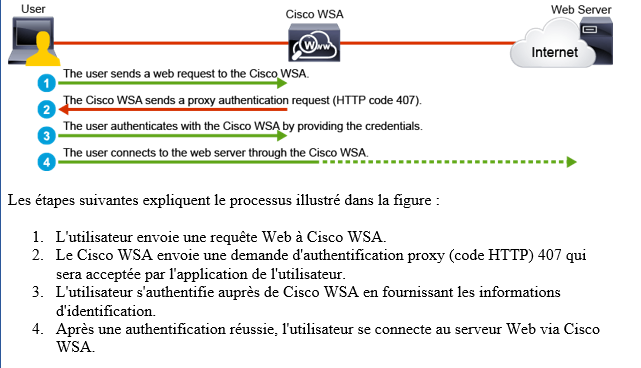
**Authentication protocols and schemes**

Cisco WSA supports two authentication protocols: NTLM and LDAP

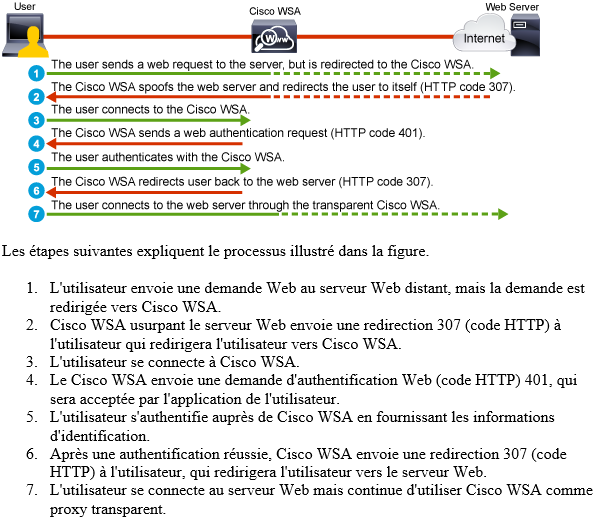
NTLM is more commonly used because of the broad usage of active directory. For NTLM authentication protocol Cisco WSA supports the following client-side authentication schemes:

* **Kerberos**: better performance and stronger authentication
* **NTLMSSP:** challenge-response sequence of messages
* **Basic**: not secure, credentials are sent as cleartext

**User Authentication in explicit proxy mode**



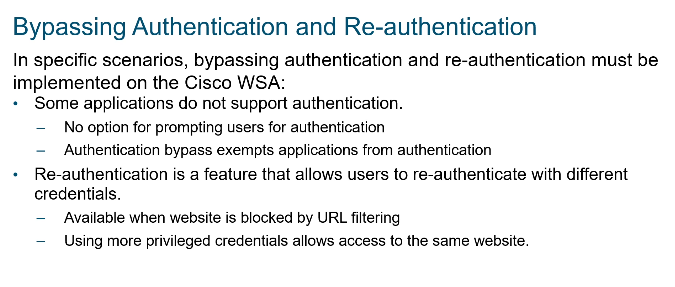
**User Authentication in transparent proxy mode**

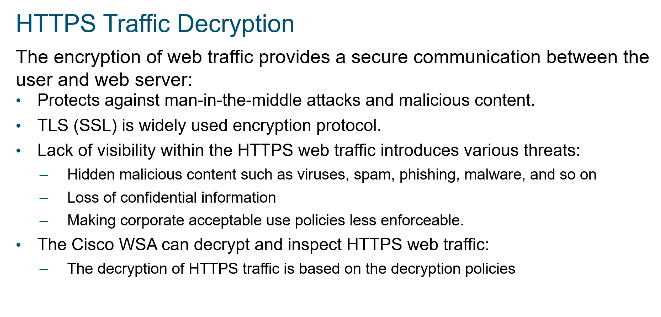


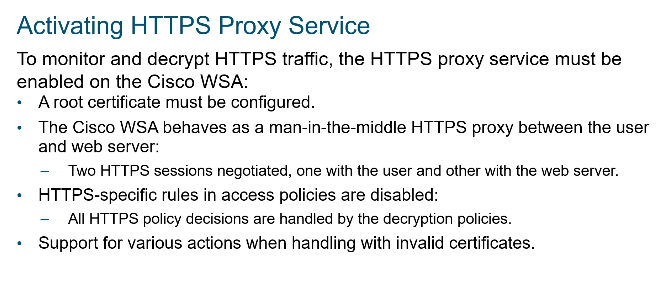
**Authentication Realms** (domaine d’authentification)

The user authentication is performed against an authentication realm configured on the cisco WSA

Cisco WSA can transparently authenticate users via cisco ISE by using the 802.1X authentication methods



**HTTPS Traffic Decryption** 

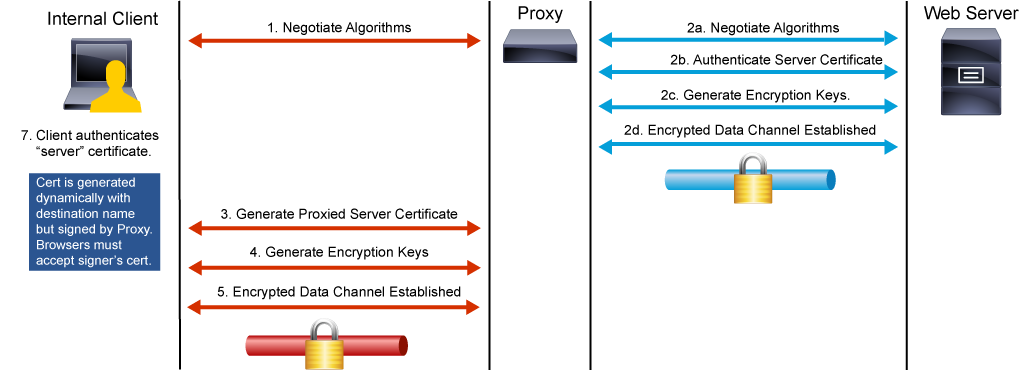


**Certificat Implementation**

* When the user initiates an HTTPS session, the server always replies with a server certificate that must be accepted by the user so the web traffic will be protected in both directions during transport.
* However, this communication is not direct between the user and web server because the Cisco WSA operates as a man-in-the-middle web proxy between them.
* Anytime the web server sends a server certificate that uniquely identifies itself, the Cisco WSA intercepts it and signs the certificate with its private key that corresponds to the root certificate that is locally used. The Cisco WSA must use a root certificate to actively generate server certificates for an HTTPS decryption.

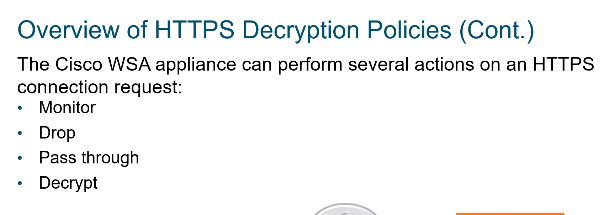
Two options are available for root certificate usage:

* **Generate a certificate and private key:** Generating a self-signed certificate and private key on the Cisco WSA
* **Upload CA root certificate and private key:** Upload into the Cisco WSA a valid root certificate and its matching private key from the trusted enterprise CA within the organization
* **Established HTTPS Sessions**



**Decryption policies can** be defined using the following control settings:

* **URL filtering:** The URL filtering provides the Cisco WSA with the option to define appropriate action for HTTPS requests for each predefined and custom URL category.
* **Web reputation:** The web reputation control setting specifies the action that the Cisco WSA should perform on the requested HTTPS connections based on the WBRS score that is assigned to the requested server.
* **Default action:** The default action defines the action that the Cisco WSA should take when none of the other control settings apply.



Antimalware protection