Aggregating ACL's Via DAP

OVERVIEW

An administrator can configure multiple DAP records to address many variables. As a result, it is possible for an authenticating user to satisfy the AAA and Endpoint attribute criteria of multiple DAP records. In consequence, Access Policy Attributes, e.g., *Web-Type or Network ACL Filters* will either be consistent or conflict throughout these policies. In this case, the authorized user will get the cumulative result across all matched DAP records.

In this *use case* example, we will focus on the aggregation of Web-Type ACLs via 2 Dynamic Access Policies (DAP); *Everyone* and *Payroll_Team*. In addition, we will depict 2 user identity types with specific resource requirements via the Clientless SSL VPN Portal. For instance, a *Director of Sales* Employee with access to standard corporate resources but denied access to payroll resources, and a *Payroll* Employee with the same level of standard access however permitted access to payroll resources.

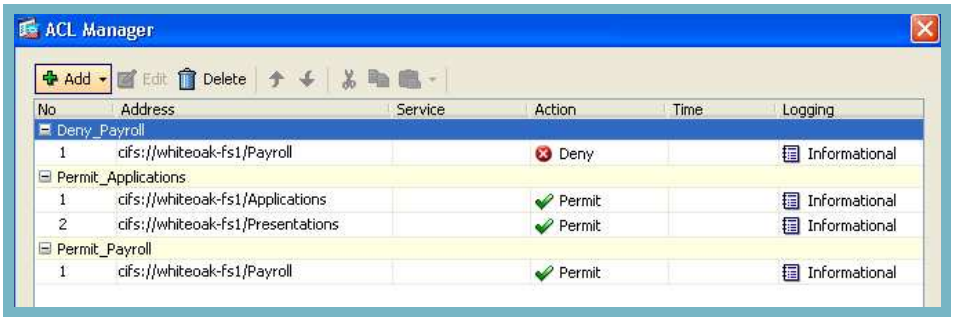
To accomplish this, we will configure both the **Director of Sales** and the **Payroll** employees to satisfy the **Everyone** DAP for access to standard corporate resources. Additionally, we will only configure **Payroll** employees to also satisfy the **Payroll_Team** DAP for additional access to *payroll resources*.

For the basis of this use case, we will assume that the required Connection Profile, Group Policy and *basic IP connectivity,* including a *DefaultDNS and AAA LDAP Server Group,* are preconfigured.

1) Defining Web-type ACLs — this configuration is necessary for defining access permits and/or denies to specific resources. We will later apply this configuration to the **Everyone** and/or **Payroll_Team** DAP for enforcement.

1. Navigate to: *Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs*, and **configure** the following:

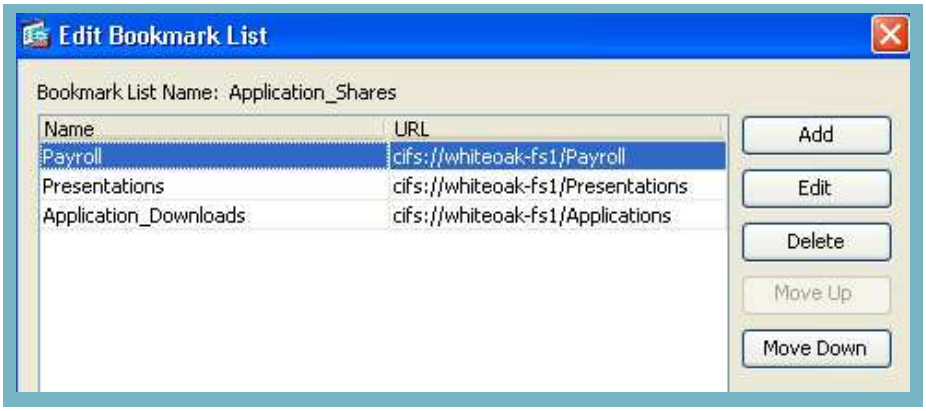
Figure 1. Web-Type ACL Filter Configuration



2) Defining Bookmark Lists — this configuration is necessary for defining Web-Type resources, e.g., CIFS shares to be accessible on the Clientless SSL VPN Portal. We will later apply this configuration to the **Everyone** and **Payroll_Team** DAP for enforcement.

1. Navigate to: *Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks*, and **configure** the following:

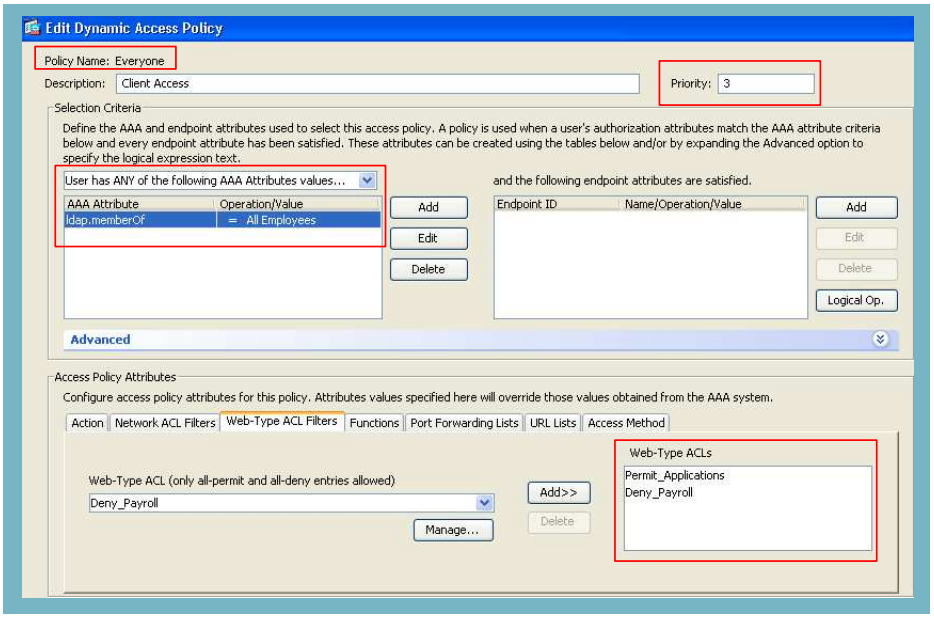
Figure 2. Bookmark List Configuration (**Application_Shares**)



3) Defining Dynamic Access Policies — this configuration is necessary for authorizing access to Access Policy Attributes, e.g., **Web-Type ACLs** as defined in Figure 1 and **URL Lists** (Bookmarks) as defined in Figure 2.

1. Navigate to: *Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies*, and **configure** the following DAP records in Figures 3 and 4:

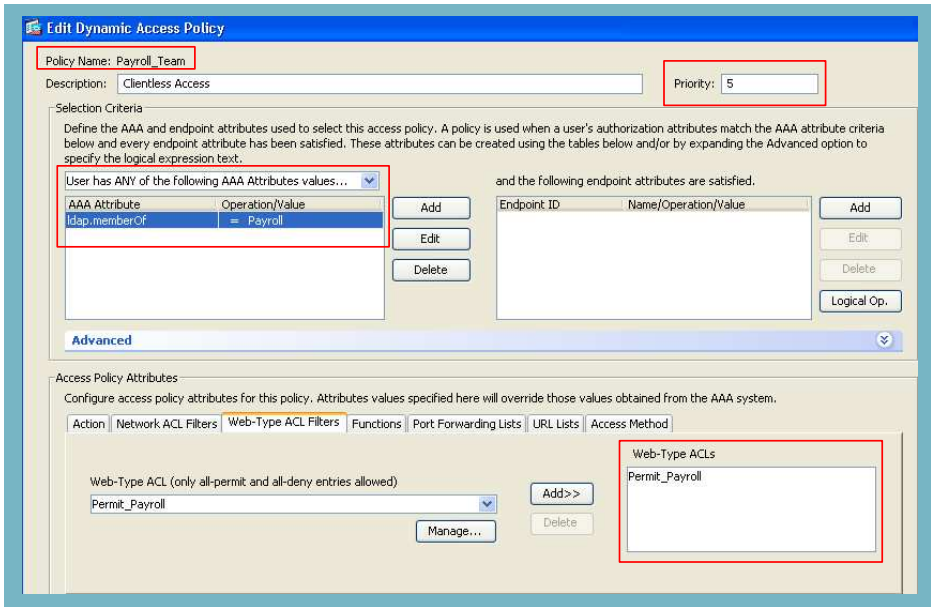
Figure 3. DAP for All Employees —The **Access Method** for this DAP is **Web-Portal** and the **URL List** applied to this DAP is **Application_Shares**)



- All employees will satisfy the Selection Criteria (**All Employees** *LDAP Attribute*) of this DAP; and will be subjected to the *Web-Type ACLs;* **Permit_Application** and **Deny_Payroll** shown in Figure 1.

- The **Priority** of **3**, will result in the Web-Type ACLs in this DAP to be ordered *after* the Web-Type ACLs in the **Payroll** DAP if both DAPS are satisfied.

Figure 4. DAP for Payroll Employees —The **Access Method** for this DAP is **Web-Portal** and the **URL List** applied to this DAP is **Application_Shares**)



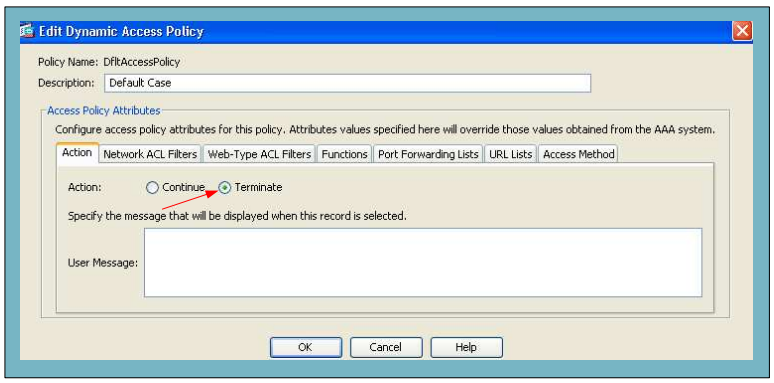
- Only payroll employees will satisfy the Selection Criteria (**Payroll** *LDAP Attribute)* of this DAP and will be subjected to the *Web-Type ACLs;* **Permit_Payroll** shown in Figure 1.

- The **Priority** of **5**, will result in the Web-Type ACLs in this DAP to be ordered ***before*** the Web-Type ACLs in the **Everyone** DAP if both DAPs are satisfied.

4) Configuring the Default DAP —to ensure that an SSL VPN connection will terminate in the default case, e.g., when the connecting employee does not match any configured Dynamic Access policies.

1. Navigate to: *Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies*, and edit the DfltAccessPolicy and configure the *Action:* attribute to **Terminate** as shown in Figure 5

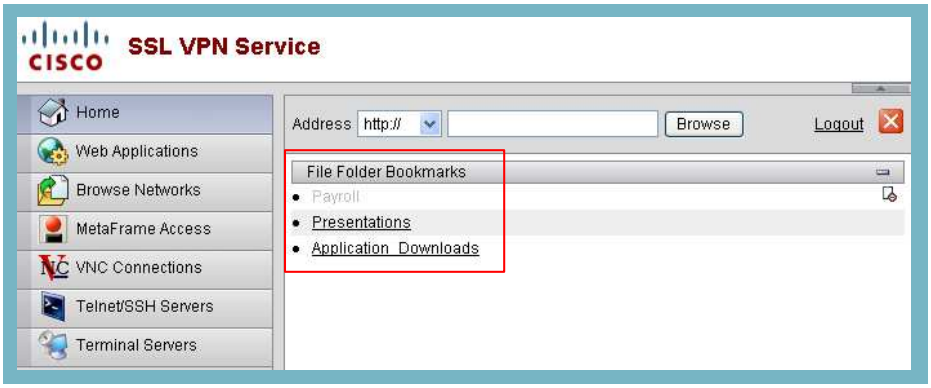
Figure 5. Dynamic Access Policy —if no predefined DAP records are matched, this DAP record will be enforced. Thus, SSL VPN access will be denied.



5) Testing your requirements —now we will establish a Clientless SSL VPN session to verify our solution. In this example, the username: **director** will represent the *Director of Sales* employee.

1. From your browser, *launch* a *Clientless SSL VPN* session with the username: **director**. Based on our configuration, this user will only satisfy the **All Employees** DAP and permitted access to the corporate standard resources; **Presentations** and **Application_Downloads** shown in Figure 6.

Figure 6. Clientless SSL VPN Session for Director of Sales Employee



Note: Because the Director of Sales employee satisfied one DAP (All Employees), Web-Type ACL aggregation does not apply. The Director will only be subjected to the Web-Type ACLs associated with this DAP. In this case, the most restrictive (Deny) ACLs will be ordered first, followed by the lease restrictive (Permit) ACLs as shown in Table 1. Note that there is an **Explicit Deny Any Any** at the end of the ACL order.

The ASA Security Appliance will enforce theses ACLs by keeping with the first-match policy.

Table 1. Web-Type ACL Attribute for Director of Sales Employee

Employee	DAPs Satisfied	Access Policy Attribute (URL Lists)	Access Policy Attribute (Web-Type ACL)
Director of Sales	All Employees	Application_Shares	Deny - Payroll
			Permit - Applications
			Permit - Presentations
			Explicit Deny Any Any

AGGREGATING ACCESS CONTROLL LISTS

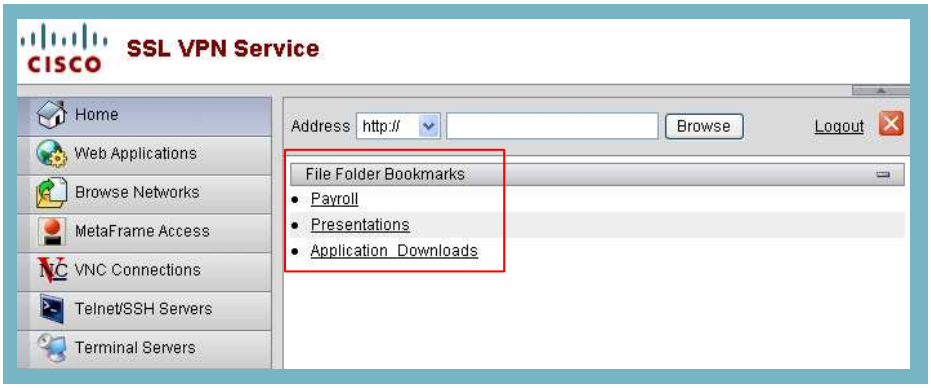
When multiple DAP records are selected, the access-lists attributes specified in the *Web-Type* (Clientless) ACL are aggregated to create a *Dynamic Access-List* for the DAP Clientless ACL.

The *Priority* attribute as shown in Figures 3 and 4 is uses to logically sequence the access lists when aggregating the Web-Type ACLs from multiple DAPs. The security appliance orders the DAPs from highest to lowest priority number, with lowest at the bottom of the table. For instance, a DAP record with a value of 5 has a higher priority than a record with a value of 3. You cannot manually sort them.

6) Testing your requirements —now we will establish a second Clientless SSL VPN session to verify our solution. In this example, the username: **payroll_user** will represent the *Payroll* employee.

1. From your browser, *launch* a *Clientless SSL VPN* session with the username: **Payroll_User**. Based on our configuration, this user will satisfy both the **All Employees** and **Payroll_Team** DAP. Thus, will be permitted access to the corporate standard resources; **Presentations** and **Application_Downloads** and **Payroll** resources shown in Figure 7.

Figure 7. Clientless SSL VPN Session for Payroll Employee



Note: Because the Payroll employee satisfied both DAPs (**All Employees** and **Payroll_Team**), Web-Type ACL aggregation will now apply. The Payroll employee will be subjected to the Web-Type ACLs associated with both DAPs.

In this case, the Security Appliance will aggregate the ACLs by first reordering the Web-Type ACLs from most restrictive to the least restrictive in the DAP with the **highest priority** number (**Payroll**), then appending the ACLs from most restrictive to the least restrictive in the DAP with the **lowest priority** number (**All Employees**) as shown in Table 2. Note that the DAP (Payroll_Team) does not have a Deny ACL, thus the least restrictive Permit ACL is ordered first. Note that there is also an **Explicit Deny Any Any** at the end of the ACL order.

The ASA Security Appliance will enforce theses ACLs by keeping with the first-match policy.

Table 2. Web-Type ACL Attribute for Payroll Employee

Employee	DAPs Satisfied	Access Policy Attribute (URL Lists)	Access Policy Attribute (Web-Type ACL)
Payroll	Payroll_Team (Priority 5)	X	Permit - Payroll
	All Employees (Priority 3)	Application_Shares	Deny - Payroll
			Permit - Applications
			Permit - Presentations
			Explicit Deny Any Any

Note: If the **Priority** number of the *Payroll_Team* DAP is **equal** or **lower** then the *All Employee* DAP, Payroll users will be denied access to payroll resources. In this case, the most restrictive Web-Type ACLs from both DAPs e.g., (**Deny - Payroll**) will be ordered first, followed by the least restrictive.

This reinforces the importance of how the Priority number of selected DAPs can affect access to corporate resources when Web-Type or Network ACLs are implemented. Please review the Dynamic Access Policy White Paper for more information on ACL aggregation.