Dynamic Access Policies

Dynamic access policies (DAP) enable you to configure authorization that addresses the dynamics of VPN environments. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security.

About Secure Firewall Threat Defense Dynamic Access Policy

VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection. For example, intranet configurations that frequently change, the various roles each user inhabits within an organization, and log in attempts from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.

You can create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group memberships and endpoint security. The threat defense grants access to a particular user for a particular session according to the policies you define. The threat defense device generates a DAP during user authentication by selecting or aggregating attributes from one or more DAP records. The device then selects these DAP records based on the endpoint security information of the remote device and AAA authorization information for the authenticated user. Then the device applies the DAP record to the user tunnel or session.

Hierarchy of Policy Enforcement of Permissions and Attributes in Threat Defense

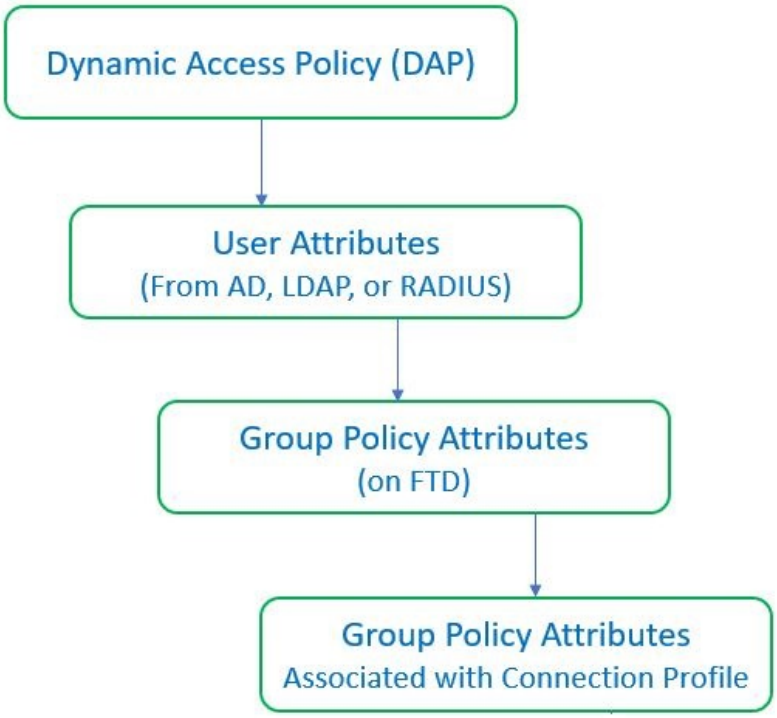
The threat defense device supports applying user authorization attributes, also called user entitlements or permissions, to VPN connections. The attributes are applied from a DAP on the threat defense, external

authentication server and/or authorization AAA server (RADIUS) or from a group policy on the threat defense device.

If the threat defense device receives attributes from all sources, the device evaluates, merges, and applies the attributes to the user policy. If there are conflicts between attributes coming from the DAP, the AAA server, or the group policy, the attributes from the DAP always take precedence.

The threat defense device applies attributes in the following order:

Figure 1: Policy Enforcement Flow



1. **DAP attributes on the FTD**—The DAP attributes take precedence over all others.
2. **User attributes on the external AAA server**—The server returns these attributes after successful user authentication and/or authorization.
3. **Group policy configured on the FTD** —If a RADIUS server returns the value of the RADIUS Class attribute IETF-Class-25 (OU= group-policy) for the user, the threat defense device places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.
4. **Group policy assigned by the Connection Profile (also known as Tunnel Group)**—The Connection Profile has the preliminary settings for the connection, and includes a default group policy that is applied to the user before authentication.

Note The threat defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. For the user session, the device uses the attributes on the group policy that you assign to the connection profile, unless the user attributes or the group policy from the AAA server overrides them.

Licensing for Dynamic Access Policies

Threat Defense must have one of the following AnyConnect Client licenses:

- AnyConnect Apex
- AnyConnect Plus
- AnyConnect VPN Only

Base license must allow export-controlled functionality.

Prerequisites for Dynamic Access Policy

Table 1:

Prerequisite Type	Description

Licensing	• Threat Defense must have at least one of the following AnyConnect Client licenses:
	  • AnyConnect Apex
	  • AnyConnect Plus
	  • AnyConnect VPN Only
	• The threat defense Base license must allow export-controlled functionality.

Configurations	For more information about prerequisites for DAP, see the *Secure Firewall Threat Defense Dynamic Access Policies* section of the *Firepower Management Center Configuration Guide*. For more information about Remote Access VPN prerequisites and configuration, see the *Secure Firewall Threat Defense Remote Access VPN* section of the *Firepower Management Center Configuration Guide*.

Guidelines and Limitations for Dynamic Access Policies

- Matching of AAA attributes in a DAP will work only if a AAA server is configured to return the correct attributes when authenticating or authorizing a remote access VPN session.
- Minimum AnyConnect and HostScan package version supported for DAP is 4.6. But it is highly recommended to use the latest version of AnyConnect.

Configure a Dynamic Access Policy (DAP)

Create a Dynamic Access Policy

Before you begin

Ensure that you have the HostScan package before you configure the dynamic access policy. You can add the HostScan file at **Objects** > **Object Management** > **VPN** > **AnyConnect File**.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy**.

Step 2 Specify the **Name** for the DAP policy and an optional **Description**.

Step 3 Select the **HostScan Package** from the list.

Step 4 Click **Save**.

What to do next

To configure DAP record, see Create a Dynamic Access Policy Record

Create a Dynamic Access Policy Record

A dynamic access policy (DAP) can contain multiple DAP records, where you configure user and endpoint attributes. You can prioritize the DAP records within a DAP so that the threat defense can select and sequence the required criteria when a user attempts VPN connection.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy**.

Step 2 Edit an existing dynamic access policy or create a new one and then edit the policy.

Step 3 Specify the **Name** for the DAP record.

Step 4 Enter the **Priority** for the DAP record.

The lower the number, the higher the priority.

Step 5 Select one of the following actions to take when a DAP record matches:

- **Continue**—Click to apply access policy attributes to the session.
- **Terminate**—Select to terminate the session.
- **Quarantine**—Select to quarantine the connection.

Step 6 Check the **Display User Message on Criterion Match** check-box and add the user message.

The threat defense displays this message to the user when the DAP record matches.

Step 7 Check the **Apply a Network ACL on Traffic** check-box and select the access control list from the drop-down.

Step 8 Check the **Apply one or more AnyConnect Custom Attributes** check-box and select the custom attributes object from the drop-down.

Step 9 Click **Save**.

Configure AAA Criteria Settings for DAP

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. The threat defense select DAP records based on the AAA authorization information for the user and posture assessment information for the session. The threat defense can choose multiple DAP records depending on this information, which it then aggregates to create DAP authorization attributes.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy**.

Step 2 Edit an existing DAP policy or create a new one and then edit the policy.

Step 3 Select a DAP record or create a new one, and edit the DAP record.

Step 4 Click **AAA Criteria**.

Step 5 Select one of the **Match criteria between sections**.

- Any—Matches any of the criteria.
- All—Matches all the criteria.
- None—Matches none of the set criteria.

Step 6 Click **Add** to add the required **Cisco VPN Criteria**.

Cisco VPN criteria include attributes for group policy, assigned IPv4 address, assigned IPv6 address, connection profile, username, username 2, and SCEP required.

a) Select an attribute and specify the **Value**.

b) Click **Add another criteria** to add more criteria.

c) Click **Save**.

SCEP Required

Step 7 Select **LDAP Criteria**, **RADIUS Criteria**, or **SAML Criteria** and specify the **Attribute ID** and **Value**.

Step 8 Click **Save**.

Configure Endpoint Attribute Selection Criteria in DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The threat defense dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database that is associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the threat defense to choose it for a session. The threat defense selects only DAP records that satisfy every condition configured.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy**.

Step 2 Edit a DAP policy and then DAP record.

Note Create a DAP policy and DAP record if not done already.

Step 3 Click **Endpoint Criteria** and configure the following endpoint criteria attributes:

Note You can create multiple instances of each type of endpoint attribute. There is no limit for the number of endpoint attributes for each DAP record.

- Add an Anti-Malware Endpoint Attribute to a DAP
- Add a Device Endpoint Attribute to a DAP
- Add AnyConnect Endpoint Attributes to a DAP, on page 8
- Add a NAC Endpoint Attribute to a DAP
- Add an Application Attribute to a DAP
- Add a Personal Firewall Endpoint Attribute to a DAP
- Add an Operating System Endpoint Attribute to a DAP
- Add a Process Endpoint Attribute to a DAP
- Add a Registry Endpoint Attribute to a DAP
- Add a File Endpoint Attribute to a DAP
- Add Certificate Authentication Attributes to a DAP

Step 4 Click **Save**.

Add an Anti-Malware Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Anti-Malware**.

Step 2 Select the Match Criteria **All** or **Any**.

Step 3 Click **Add** to add anti-malware attributes.

Step 4 Click **Installed** to indicate whether the selected endpoint attribute and its accompanying qualifiers are installed or not installed.

Step 5 Choose **Enabled** or **Disabled** to activate or deactivate real-time malware scanning.

Step 6 Select the name of the anti-malware **Vendor** from the list.

Step 7 Select the anti-malware **Product Description**.

Step 8 Choose the **Version** of the anti-malware product.

Step 9 Specify the number of days since the **Last Update**.

You can indicate that an anti-malware update must occur in less than (<) or more than (>) the number of days you specify.

Step 10 Click **Save**.

Add a Device Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and choose **Endpoint Criteria** > **Device**.

Step 2 Select the Match Criteria **All** or **Any**.

Step 3 Click **Add** and select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter for the following attributes:

- **Host Name**—Hostname of the device you are testing for. Use the computer's host name only, not the fully qualified domain name (FQDN).
- **MAC Address**—MAC address of the network interface card you are testing for. The address must be in the format xxxx.xxxx.xxxx where x is a hexadecimal character.
- **BIOS Serial Number**—BIOS serial number value of the device you are testing for. The number format is manufacturer-specific.
- **Port Number**—Listening port number of the device.
- **Secure Desktop Version**—Version of the Host Scan image running on the endpoint.
- **OPSWAT Version**—The OPSWAT client version.
- **Privacy Protection**—None, Cache cleaner, Secure Desktop.
- **TCP/UDP Port Number**—TCP or UDP port in the listening state that you are testing for.

Step 4 Click **Save**.

Add AnyConnect Endpoint Attributes to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **AnyConnect**.

Step 2 Select the Match Criteria **All** or **Any**.

Step 3 Click **Add** and select the = or ≠ operator to check the attribute to be equal to or not equal to the value you enter.

Step 4 Select the **Client Version** and **Platform**.

Step 5 Select the **Platform Version**, and specify the **Device Type** and **Device Unique ID**.

Step 6 Add the **MAC Addresses** the MAC Address Pool.

Note The MAC Address must be in the format XX-XX-XX-XX-XX-XX, where each X is a hexadecimal character. You can click **Add another MAC Address** to add more addresses.

Step 7 Click **Save**.

Add NAC Endpoint Attributes to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **NAC**.

Step 2 Select the Match Criteria **All** or **Any**.

Step 3 Click **Add** to add NAC attributes.

Step 4 Set the operator to be equal to = or not equal to ≠ the posture token string. Enter the posture token string in the **Posture Status** box.

Step 5 Click **Save**.

Add an Application Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Application**.

Step 2 Select the Match Criteria **All** or **Any**.

Step 3 Click **Add** to add application attributes.

Step 4 Choose equals (=) or does not equal (≠) and specify the **Client Type** to indicate the type of remote access connection.

Step 5 Click **Save**.

Add a Personal Firewall Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Personal Firewall**.
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add personal firewall attributes.
Step 4 Click **Installed** to indicate whether the personal firewall endpoint attribute and its accompanying qualifiers (fields below the Name/Operation/Value column) are installed or not installed.
Step 5 Choose **Enabled** or **Disabled** to activate or deactivate firewall protection.
Step 6 Select the name of the firewall **Vendor** from the list.
Step 7 Select the firewall **Product Description**.
Step 8 Select the equals (=) or does not equal (≠) operator and choose the **Version** of the personal firewall product.
Step 9 Click **Save**.

Add an Operating System Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Operating System** .
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add endpoint attributes.
Step 4 Select the equals (=) or does not equal (≠) operator and then select the **Operating System**.
Step 5 Select the equals (=) or does not equal (≠) operator and then specify the operating system **Version**.
Step 6 Click **Save**.

Add a Process Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Process**.
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add the process attributes.
Step 4 Select **Exists** or **Does not exist**.
Step 5 Specify the **Process Name**.

Step 6 Click **Save**.

Add a Registry Endpoint Attribute to a DAP

Scanning for registry endpoint attributes applies to Windows operating systems only.

Before you begin

Before configuring a Registry endpoint attribute, define the registry key for which you want to scan in the Host Scan window for Cisco Secure Desktop.

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Registry**.
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add registry attributes.
Step 4 Select the **Entry Path** for the registry and specify the path.
Step 5 Choose the existence of the registry, **Exists** or **Does not Exist**.
Step 6 Select the registry **Type** from the list.
Step 7 Select the equals (=) or does not equal (≠) operator and enter the **Value** of the registry key.
Step 8 Select **Case insensitive** to disregard the case of the registry entry while scanning.
Step 9 Click **Save**.

Add a File Endpoint Attribute to a DAP

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **File**.
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add file attributes.
Step 4 Specify the **File Path**.
Step 5 Choose **Exists** or **Does not exist** to indicate the presence of the file.
Step 6 Select less than (<) or greater than (>) and specify the **Last Modified** days for the file.
Step 7 Select the equal to (=) or not equal to ≠ operator and enter the **Checksum**.
Step 8 Click **Save**.

Add Certificate Authentication Attributes to a DAP

You can index each certificate to allow referencing to any of the received certificates, by the configured rules. Based on these certificate fields, you can configure DAP rules to allow or disallow connection attempts.

Procedure

Step 1 Edit a DAP record and select **Endpoint Criteria** > **Certificate**.
Step 2 Select the Match Criteria **All** or **Any**.
Step 3 Click **Add** to add certificate attributes.
Step 4 Select the certificate **Cert1** or **Cert2**.
Step 5 Select the **Subject** and specify the subject value.
Step 6 Select the **Issuer** and specify the issuer value.
Step 7 Select the **Subject Alternate Name** and specify the subject value.
Step 8 Specify the **Serial Number**.
Step 9 Choose the **Certificate Store**: None, Machine, or User.

The VPN client sends the certificate store information.

Step 10 Click **Save**.

Configure Advanced Settings for DAP

You can use the Advanced tab for adding selection criteria other than what is possible in the AAA and endpoint attribute areas. For example, while you can configure the threat defense to use AAA attributes that satisfy any, all, or none of the specified criteria, the endpoint attributes are cumulative, and must satisfy all. To let the security appliance employ one endpoint attribute or another, you must create appropriate logical expressions in Lua and enter them here.

Procedure

Step 1 Choose **Devices** > **Dynamic Access Policy**.
Step 2 Edit a DAP policy and then edit a DAP record.

Note Create a DAP policy and DAP record if not done already.

Step 3 Click the **Advanced** tab.
Step 4 Select **AND** or **OR** as the match criteria to use in the DAP configuration.
Step 5 Add the Lua script in the **Lua script for advanced attribute matching** field.
Step 6 Click **Save**.

Associate Dynamic Access Policy with Remote Access VPN

You can associate Dynamic Access Policy (DAP) with remote access VPN policy for the dynamic access policy attributes to match during VPN session authentication and authorization. You can then deploy the remote access VPN on the threat defense.

Procedure

Step 1 Choose **Devices** > **Remote Access**.

Step 2 Click **Edit** next to the remote access VPN policy to which you want to associate dynamic access policy.

Step 3 Click the link in remote access VPN to select the dynamic access policy.

Step 4 Select the policy from the **Dynamic Access Policy** drop-down or click **Create a new Dynamic Access Policy** to configure a new dynamic access policy.

Step 5 Click **OK**.

Step 6 Click **Save** to save the remote access VPN policy.

When the remote access VPN user tries to connect, the VPN checks the configured dynamic access policy records and attributes. VPN creates a dynamic access policy based on the matching dynamic access policy records and takes appropriate action on the VPN session.

History for Dynamic Access Policy

Feature	Version	Minimum Threat Defense	Details
Dynamic Access Policy	7.0	Any	The feature was introduced.