Firepower Threat Defense Dynamic Access Policies Overview

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 Firepower 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 may inhabit within an organization, and logins 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 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. That is, the FTD grants access to a particular user for a particular session based on the policies you define. It generates a DAP during user authentication by selecting or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.

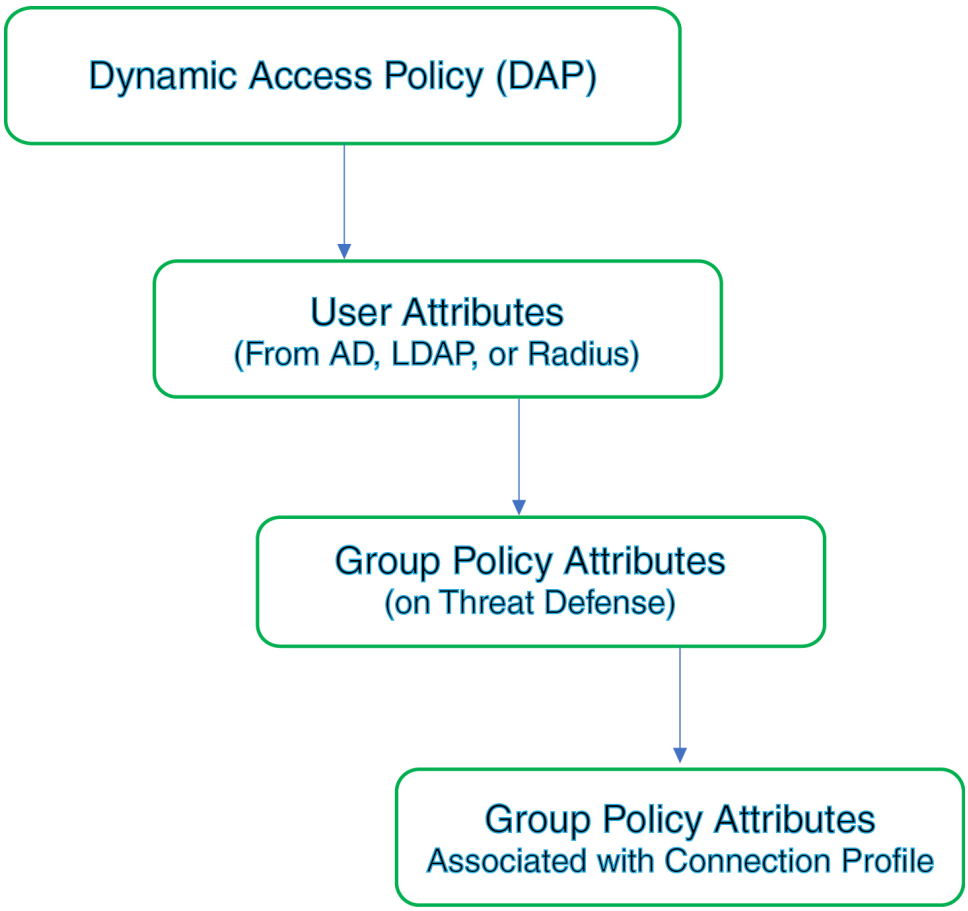
Policy Enforcement of Permissions and Attributes in FTD

The Firepower 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

457903Firepower Threat Defense, external authentication server and/or authorization AAA server (RADIUS) or from a group policy on the Firepower Threat Defense device.

If the Firepower Threat Defense device receives attributes from all sources, Firepower Threat Defense evaluates, merges, and applies to the user policy. If conflicts occur among attributes coming from the DAP, the AAA server, or the group policy, the attributes obtained from the DAP always take precedence.

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 Firepower 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 applied to the user before authentication.

Note The Firepower Threat Defense device does not support inheriting system default attributes from the default group policy, *DfltGrpPolicy*. The group policy attributes assigned from the connection profile are used for the user session, if they are not overridden by user attributes or the group policy from the AAA server.

Licensing for Dynamic Access Policies

FTD must have one of the following AnyConnect 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	• FTD must have at least one of the following AnyConnect licenses:
	  • AnyConnect Apex
	  • AnyConnect Plus
	  • AnyConnect VPN Only
	• The FTD base license must allow export-controlled functionality.

Configurations	For more information about prerequisites for DAP, see the *Firepower 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 *Firepower 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

You must create a DAP policy and then add a configure the attributes for the policy.

Before you begin

Ensure that you have the HostScan package before configuring DAP endpoint attributes. 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**.

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 required criteria is applied when a user attempts a VPN connection.

For information about DAP records for specific scenarios, see Firepower Threat Defense Dynamic Access Policy Use Cases.

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

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

Step 5 Select an Action to be taken when 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 Select **Display User Message on Criterion Match** and add the message in the box.

The message is displayed to the user when this DAP record is selected.

Step 7 Select the **Apply a Network ACL on Traffic** checkbox and select the ACL from the list.

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

Step 9 Click **Save**.

Configure AAA Criteria Settings for a DAP

DAP complements AAA services by providing a limited set of authorization attributes that can override the attributes that AAA provides. The FTD selects DAP records based on the AAA authorization information for the user and posture assessment information for the session. The FTD 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 of the criteria
- None—matches none of the set criteria

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

Cisco VPN Criteria includes 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 a DAP

Endpoint attributes contain information about the endpoint system environment, posture assessment results, and applications. The FTD dynamically generates a collection of endpoint attributes during session establishment and stores these attributes in a database associated with the session. Each DAP record specifies the endpoint selection attributes that must be satisfied for the FTD to choose it for a session. The FTD 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 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 de-activate 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 should 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 select **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**—Host name 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 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 anti-malware attributes.

Step 4 Choose equals (=) or does not equal (≠) and specify the **Client Type** 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 anti-malware attributes.
Step 4 Click **Installed** to indicate whether the selected 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 de-activate 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 anti-malware 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 anti-malware 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

Before you begin

Before configuring a File endpoint attribute, define the file 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** > **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 equals (=) or does not equal ≠ operator and enter the **Checksum**.
Step 8 Click **Save**.

Add Certificate Authentication Attributes to DAP

You can index each certificate so that any of the received certificates can be referenced 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 anti-malware 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 Select the **Certificate Store**: None, Machine, or User.

This information is sent by the VPN client.

Step 10 Click **Save**.

Configure Advanced Settings for a 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 FTD to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative, and must all be satisfied. To let the security appliance employ one endpoint attribute or another, you need to 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 Select **AND** or **OR** as the match criteria to be performed on DAP configuration.

Step 4 Add the **Lua script for advanced attribute matching**.

Step 5 Click **Save**.

Associate a DAP with a Remote Access VPN

A dynamic access policy must be associated with a remote access VPN policy for the DAP attributes to match during VPN session authentication and authorization. You can then deploy the remote access VPN on FTD.

Procedure

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

Step 2 Select an existing remote access VPN policy or create a new one.

Step 3 Edit a remote access VPN policy.

Step 4 Click the link in remote access VPN to select the Dynamic Access Policy.

Step 5 Select the **Dynamic Access Policy** from the list or click Add to configure a new DAP policy.

Step 6 Click **OK**.

Step 7 Click **Save** to save the remote access VPN policy.

Once you associate a dynamic access policy to a remote access VPN, the configured DAP records and attributes are checked when a VPN user tries to connect to the VPN. A DAP is created based on the matching and the appropriate action is taken on the VPN session.

History for Dynamic Access Policy

Feature	Version	Details
Dynamic Access Policy	7.0	The feature was introduced.