Configure Custom File-Filtering Profiles

For supported software information, click here.

On Versa Operating System^{TM} (VOS^{TM}) devices, you can use file filtering to reduce the risk of attacks from unwanted and malicious files, thus decreasing an attacker's ability to attack your organization by protecting against virus and vulnerabilities that are associated with various types of files. File filtering is performed based on the file type and the hash of the file.

You can configure file filtering to block the transfer of potentially dangerous files and types of files (that is, files associated with specific applications), files of specific sizes, files associated with specific protocols, and files traveling in a particular direction. You can configure SHA-based hash lists of files to mark potentially dangerous files for denying (sometimes called blacklisting) and to mark safe files for allowing (sometimes called whitelisting). You can configure file filtering to perform reputation-based file hash lookups on a cloud server.

Deny list, allow list, and cloud lookup file-filtering scans calculate the SHA-256 and SHA-384 sums of the file. You can configure a deny or a allow to match the SHA-256 and SHA-384 sums.

To configure file filtering, you create a file-filtering profile that defines rules for filtering files that enter and leave the network. The rules define match conditions and actions to take when a file does or does not meet the match conditions. You associate file filtering profiles with devices that are connected to a Secure Web Gateway (SWG) and that need to send traffic to the internet.

The file-filtering process is performed in the following sequence:

1. Scan the early bytes of an incoming file and identify the file type.
2. Calculate the SHA-256 or SHA-384 sum (or both) of the file and check whether it matches a deny list or an allow list entry.
    a. If a deny list entry matches, take the action configured in the deny list rule.
    b. If no deny list entry matches, check the allow list entries.
    c. If an allow list entry matches, take the action configured in the allow list rule.
    d. If no deny list or allow list entries match, check the configured rules.
3. Search the configured rules to check whether the file type, file size, protocol, and direction match one of the rules.
    a. If a match occurs, take the appropriate rule action.
    b. If no match occurs, perform a cloud lookup.
4. Perform a cloud lookup, sending the hash of the file, to check the file's reputation.

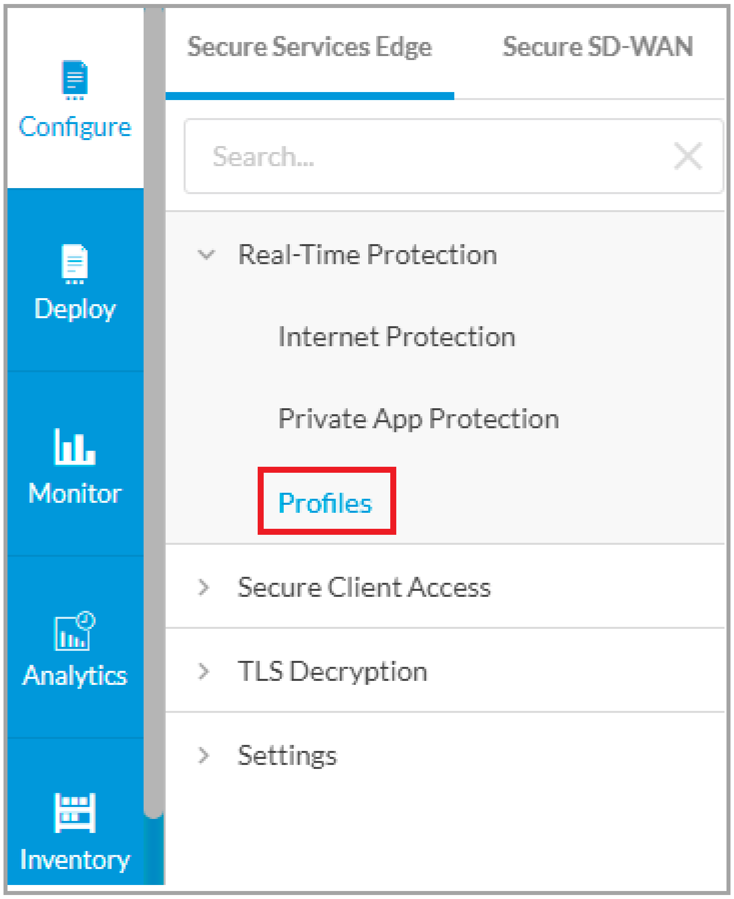
Copyright © 2024, Versa Networks, Inc.

   a. If the hash of the file is found, take the configure action. A hash can indicate that the file is clean, malicious, or suspicious.

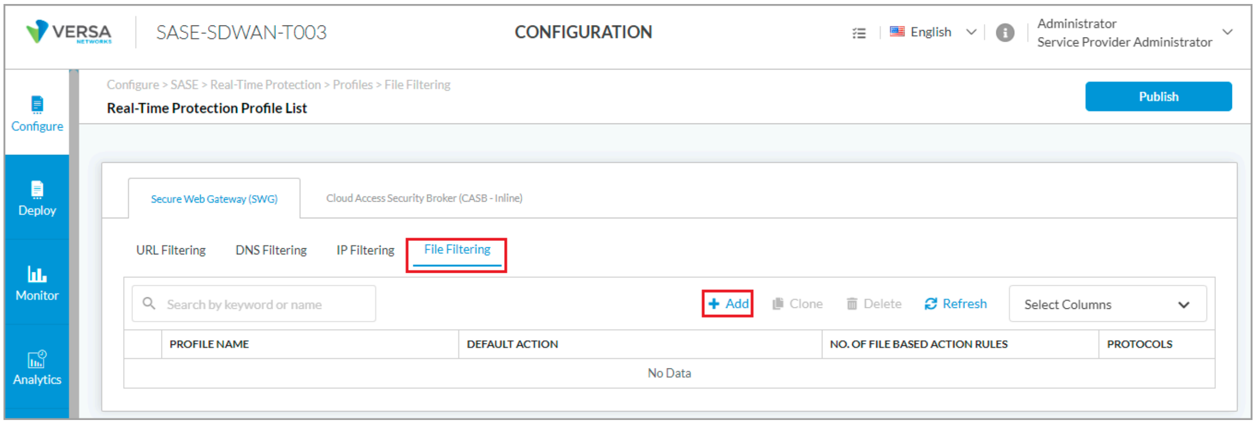
5. If the file matches none of these, take the default action defined in the file-filtering profile.

To configure custom file-filtering profiles:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



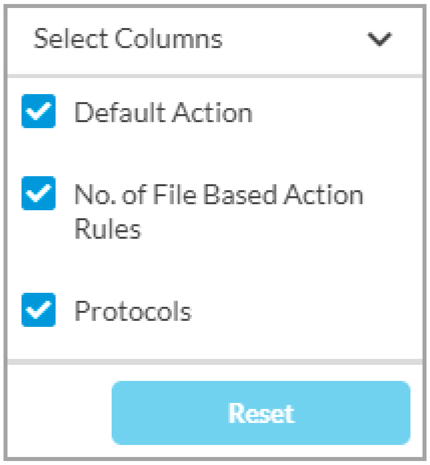
   The following screen displays:



	PROFILE NAME	DEFAULT ACTION	NO. OF FILE BASED ACTION RULES	PROTOCOLS
		No Data		

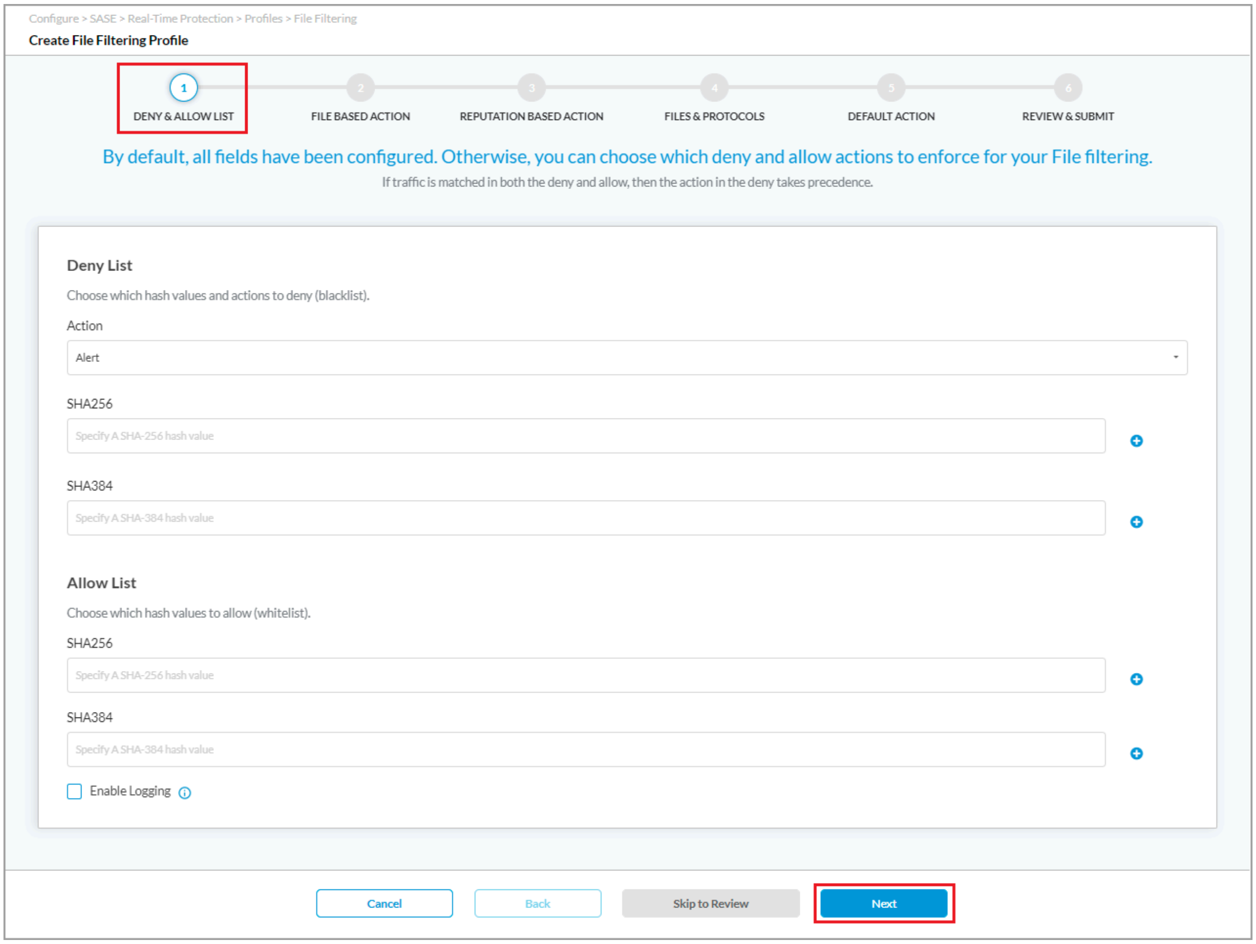
Copyright © 2024, Versa Networks, Inc.

2. Select Secure Web Gateway (SWG) > File Filtering tab.
3. To customize which columns display, click Select Columns and then click the columns to select or deselect the one you want to display. Click Reset to return to the default column display settings.



4. Click + Add to create a profile. The Create IP Filtering screen displays, and the Deny and Allow List step selected. By default, all fields are configured. To customize IP filtering actions, enter information for the following fields. Note that if the traffic matches both a deny list and an allow list, the action in the deny list takes precedence.

Copyright © 2024, Versa Networks, Inc.



Configure > SASE > Real-Time Protection > Profiles > File Filtering

Create File Filtering Profile

By default, all fields have been configured. Otherwise, you can choose which deny and allow actions to enforce for your File filtering.

If traffic is matched in both the deny and allow, then the action in the deny takes precedence.

Deny List

Choose which hash values and actions to deny (blacklist).

Action: Alert

SHA256: Specify A SHA-256 hash value

SHA384: Specify A SHA-384 hash value

Allow List

Choose which hash values to allow (whitelist).

SHA256: Specify A SHA-256 hash value

SHA384: Specify A SHA-384 hash value

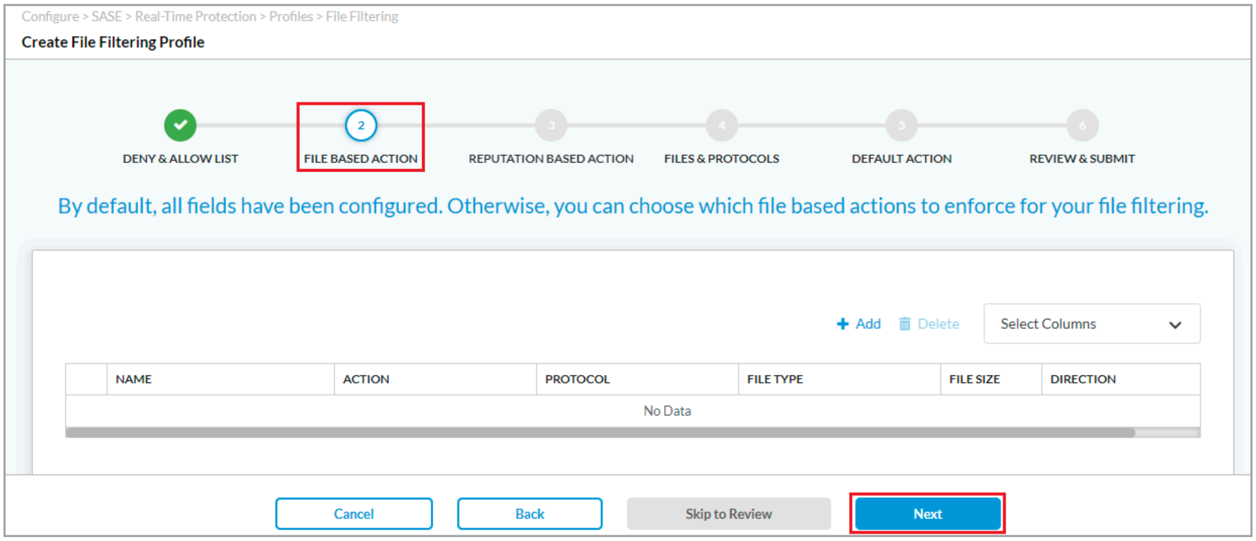
☐ Enable Logging

Field	Description
Deny List (Group of Fields)	Configure a SHA-based list of files to deny.
◦ Action	Select the default action to take when a file is detected in the deny list: ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Block—Do not allow the file to pass and, if a LEF profile is configured, log the acti ◦ Reject—Reset the connection to the server and client and, if a LEF profile is confi
◦ SHA256	Click the + Add icon to specify the SHA-256 hash value of a denied file. You can ass with a file for the deny list check.

Copyright © 2024, Versa Networks, Inc.

◦ SHA384	Click the + Add icon to specify the SHA-384 hash value of a denied file. You can ass with a file for the deny check.
Allow List (Group of Fields)	
◦ SHA256	Click the + Add icon to specify the SHA-256 hash value of an allowed file. You can a value with a file for the allow list check.
◦ SHA384	Click the + Add icon to specify the SHA-384 hash value of an allowed file. You can a value with a file for the allow list check.
◦ Enable Logging	Select to store logs for allowed files.

5. Click Next to go to the File-Based Action screen, to configure file-filtering rules for file properties, such as file type, file size, protocol, and direction.



Configure > SASE > Real-Time Protection > Profiles > File Filtering

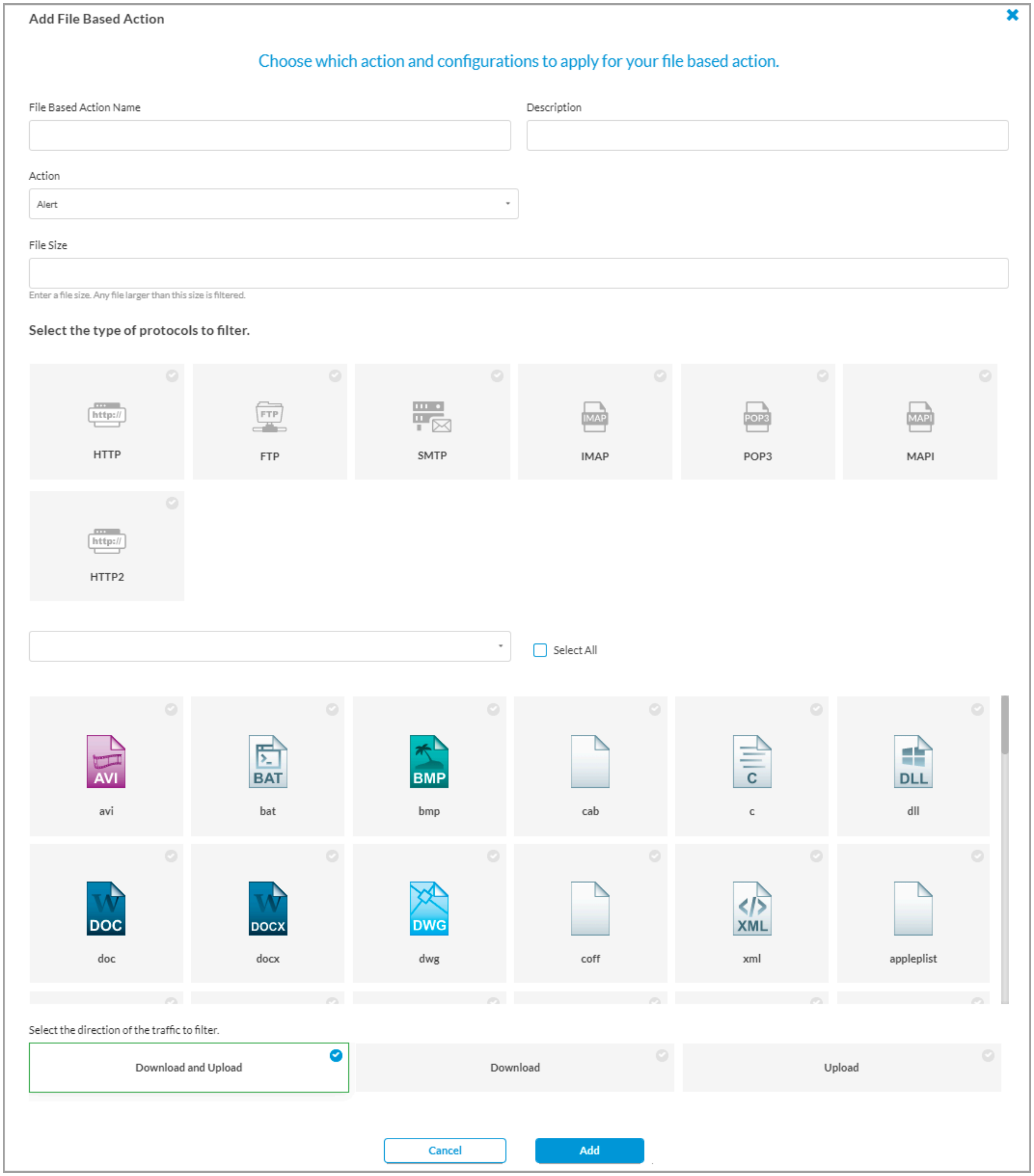
Create File Filtering Profile

By default, all fields have been configured. Otherwise, you can choose which file based actions to enforce for your file filtering.

NAME	ACTION	PROTOCOL	FILE TYPE	FILE SIZE	DIRECTION
No Data					

6. Click + Add icon, and in the Add File-Based Action popup window, enter information for the following fields.

Copyright © 2024, Versa Networks, Inc.



Add File Based Action

Choose which action and configurations to apply for your file based action.

File Based Action Name

Description

Action

Alert

File Size

Enter a file size. Any file larger than this size is filtered.

Select the type of protocols to filter.

□ Select All

Select the direction of the traffic to filter.

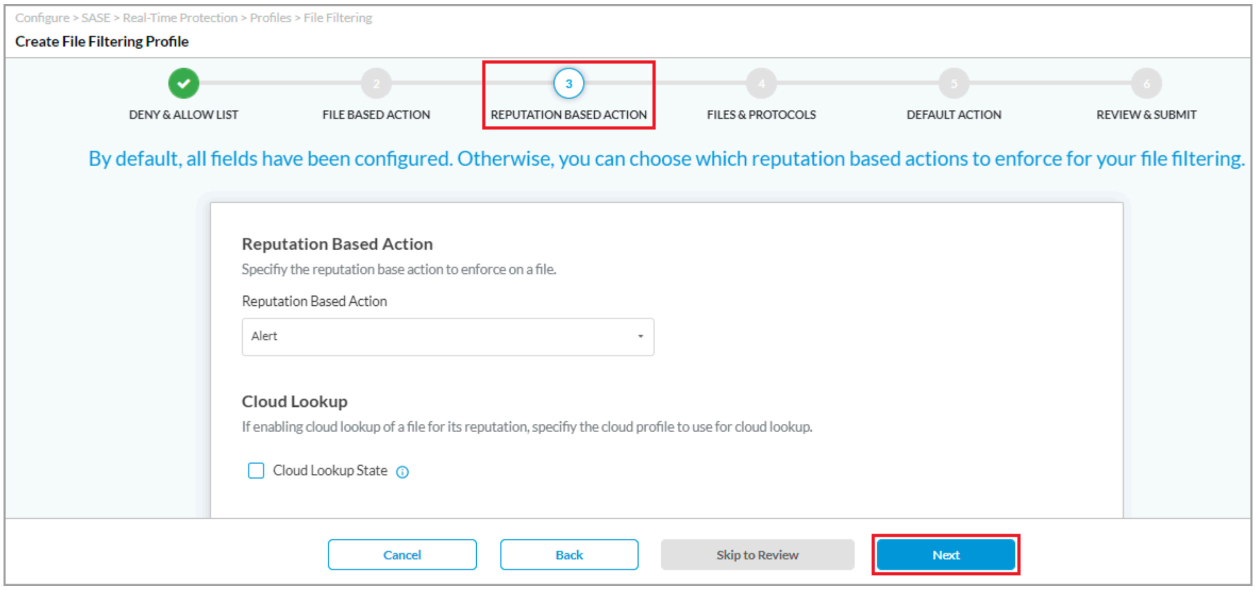
Copyright © 2024, Versa Networks, Inc.

Field	Description
File-Based Action Name	Enter a name for the file action.
Description	Enter a text description for the file action.
Action	Select the default action to take on a file: ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Allow—Allow the file to pass without logging the action. ◦ Block—Do not allow the file to pass and, if a LEF profile is configured, log the action. ◦ Reject—Reset the connection to the server and client and, if a LEF profile is configured, log the action.
File Size	Enter a file size. Any file larger than this size is filtered. *Value*: 1 through 4294967295 *Default*: None
Select the type of protocols to filter	Select the protocols to associate with the file transfer. You can select multiple protocols.
Select files	Select the file type on which to apply the file filter. You can select multiple file types or click Select All to select all files.
Select the direction of the traffic to filter	Select the direction in which to apply the file filter: ◦ Download and upload ◦ Download ◦ Upload

7. Click Add.
8. Click Next to go to the Reputation-Based Action screen to configure file-filtering rules for cloud-based hash

Copyright © 2024, Versa Networks, Inc.

lookups. Enter information for the following fields.


Configure > SASE > Real-Time Protection > Profiles > File Filtering

Create File Filtering Profile

By default, all fields have been configured. Otherwise, you can choose which reputation based actions to enforce for your file filtering.

Reputation Based Action

Specifiy the reputation base action to enforce on a file.

Reputation Based Action: Alert

Cloud Lookup

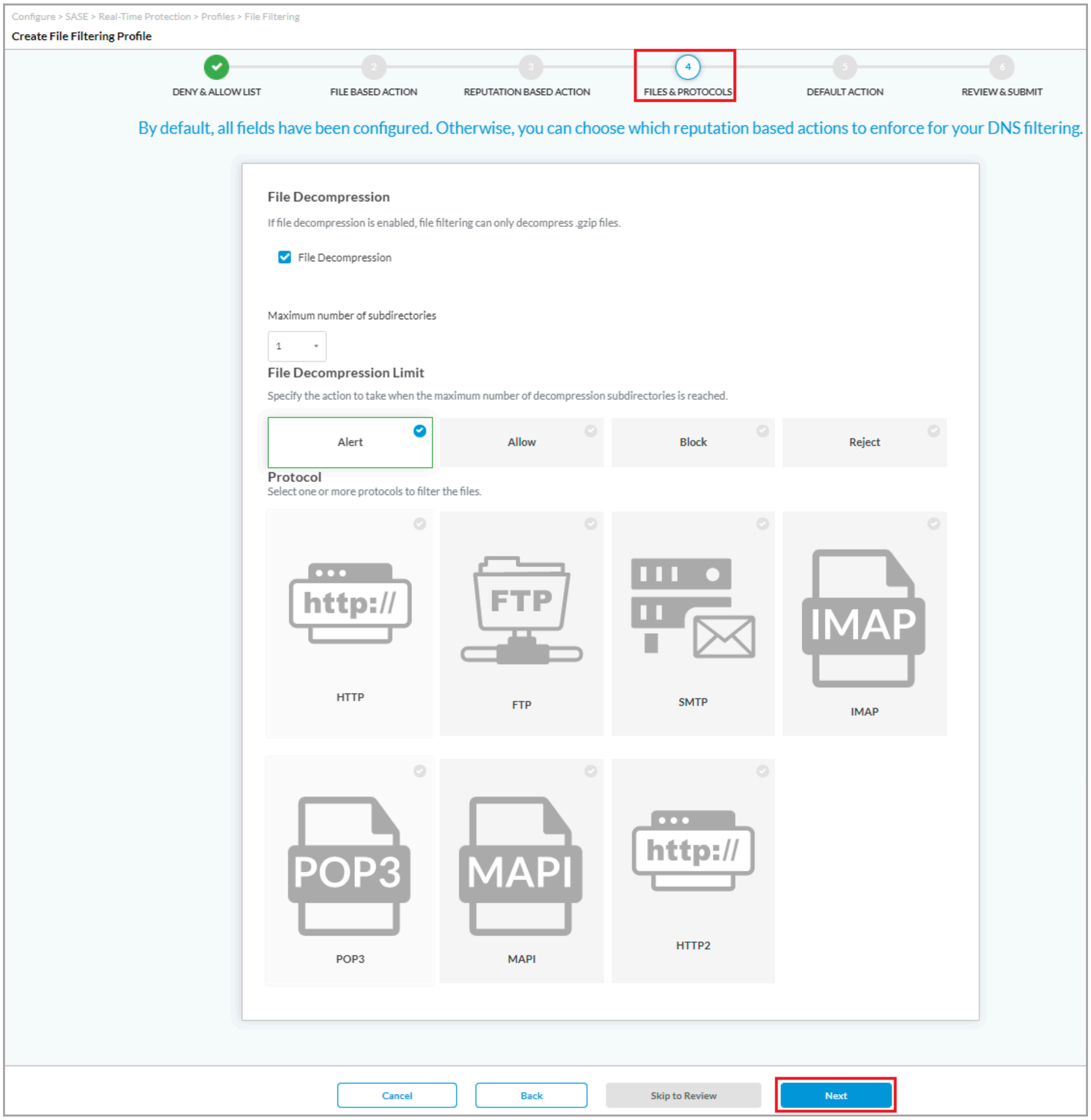
If enabling cloud lookup of a file for its reputation, specify the cloud profile to use for cloud lookup.

□ Cloud Lookup State

Field	Description
Action	Select the default action to take on a file: ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Allow—Allow the file to pass without logging the action. ◦ Block—Do not allow the file to pass and, if a LEF profile is configured, log the action. ◦ Reject—Reset the connection to the server and client and, if a LEF profile is configured, log the action.
Cloud Lookup State	Click to enable cloud lookup of a file for its reputation.

9. Click Next to go to the Files and Protocols screen, to select the default action to perform when there is no matching criteria. Enter information for the following fields.

Copyright © 2024, Versa Networks, Inc.



Configure > SASE > Real-Time Protection > Profiles > File Filtering

Create File Filtering Profile

By default, all fields have been configured. Otherwise, you can choose which reputation based actions to enforce for your DNS filtering.

File Decompression

If file decompression is enabled, file filtering can only decompress .gzip files.

☑ File Decompression

Maximum number of subdirectories

1

File Decompression Limit

Specify the action to take when the maximum number of decompression subdirectories is reached.

Protocol

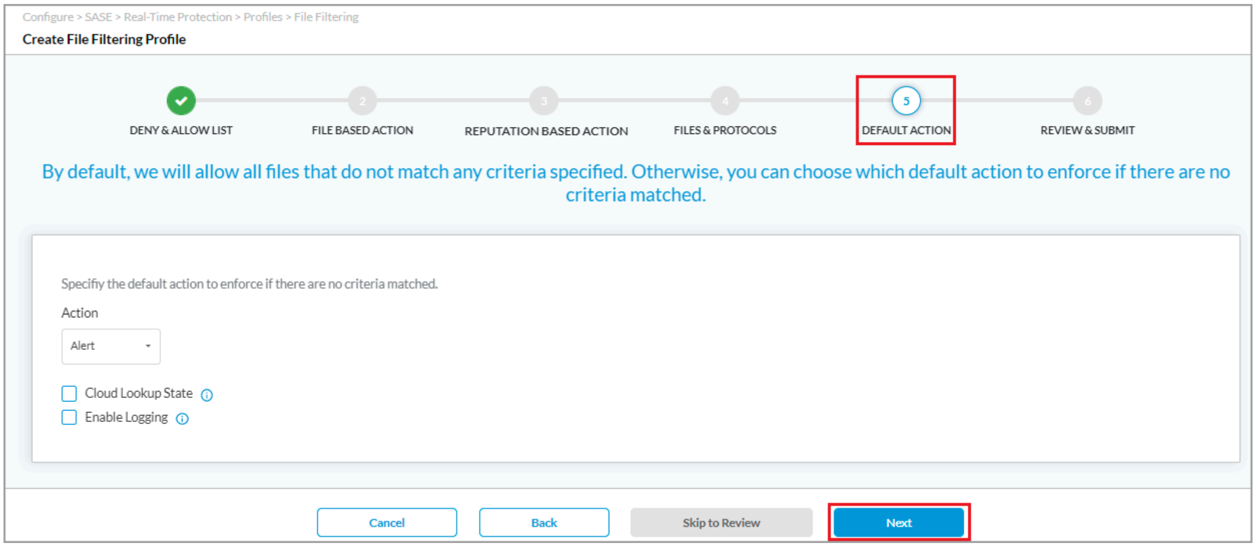
Select one or more protocols to filter the files.

Copyright © 2024, Versa Networks, Inc.

Field	Description
File Decompression (Group of Files)	Configure file decompression. Note that file filtering can decompress only .gzip files.
◦ File Decompression	Click to decompress the files being filtered and to place them into subdirectories.
◦ Maximum Number of Subdirectories	Enter the maximum number of subdirectories. Note that a .gzip file can be decompressed only into a single subdirectory. *Range*: 1 through 10 *Default*: 1
Specify the action	Select the action to take when the maximum number of decompression subdirectories is reached: ◦ Alert ◦ Allow ◦ Block ◦ Reject
◦ Protocol	Select one or more protocols to filter the files: ◦ FTP ◦ HTTP ◦ IMAP ◦ MAPI ◦ POP3 ◦ SMTP

10. Click Next to go to the Default Action screen, and enter information for the following fields.

Copyright © 2024, Versa Networks, Inc.



By default, we will allow all files that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Specifiy the default action to enforce if there are no criteria matched.

Action: Alert

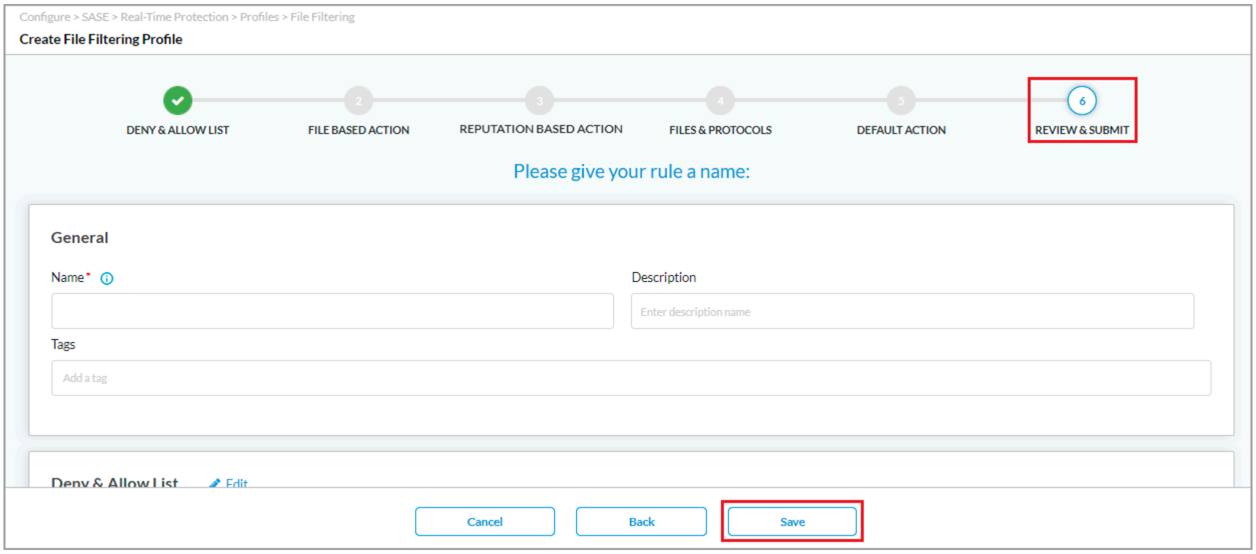
□ Cloud Lookup State

□ Enable Logging

Field	Description
Action	Select the default action to take on a file: ◦ Alert—Allow the file to pass and, if a LEF profile is configured, log the action. ◦ Allow—Allow the file to pass without logging the action. ◦ Block—Do not allow the file to pass and, if a LEF profile is configured, log the action. ◦ Reject—Reset the connection to the server and client and, if a LEF profile is configured, log the action.
Cloud Lookup	Click to enable cloud lookup of a file for its reputation.
Enable Logging	Click to store logs.

11. Click Next to go to the Review and Submit screen.

Copyright © 2024, Versa Networks, Inc.



Configure > SASE > Real-Time Protection > Profiles > File Filtering

Create File Filtering Profile

Please give your rule a name:

General

Name*

Description: Enter description name

Tags: Add a tag

Deny & Allow List ✎ Edit

12. In the General section, enter a name for the File filtering profile and, optionally, a description and tags.
13. For all other sections, review the information. If you need to make changes, click the Edit icon.
14. Click Save.

To delete a file filtering profile, select the profile in the File Filtering tab and click the 🗑 Delete Delete icon.

Supported Software Information

Releases 11.2.1 and later support all content described in this article.

Additional Information

[Configure Custom URL-Filtering Profiles]

[Configure SASE Internet Protection Rules]

Copyright © 2024, Versa Networks, Inc.