ASA and Cisco Cloud Web Security

Cisco Cloud Web Security (also known as ScanSafe) provides web security and web filtering services through the Software-as-a-Service (SaaS) model. Enterprises with the ASA in their network can use Cloud Web Security services without having to install additional hardware.

Information About Cisco Cloud Web Security

When you enable Cloud Web Security on the ASA, the ASA transparently redirects selected HTTP and HTTPS traffic to the Cloud Web Security proxy servers based on service policy rules. The Cloud Web Security proxy servers then scan the content and allow, block, or send a warning about the traffic based on the policy configured in Cisco ScanCenter to enforce acceptable use and to protect users from malware.

The ASA can optionally authenticate and identify users with Identity Firewall and AAA rules. The ASA encrypts and includes the user credentials (including usernames and user groups) in the traffic it redirects to Cloud Web Security. The Cloud Web Security service then uses the user credentials to match the traffic to the policy. It also uses these credentials for user-based reporting. Without user authentication, the ASA can supply an (optional) default username and group, although usernames and groups are not required for the Cloud Web Security service to apply policy.

You can customize the traffic you want to send to Cloud Web Security when you create your service policy rules. You can also configure a “whitelist” so that a subset of web traffic that matches the service policy rule instead goes directly to the originally requested web server and is not scanned by Cloud Web Security.

You can configure a primary and a backup Cloud Web Security proxy server, each of which the ASA polls regularly to check for availability.

User Identity and Cloud Web Security

You can use user identity to apply policy in Cloud Web Security. User identity is also useful for Cloud Web Security reporting. User identity is not required to use Cloud Web Security. There are other methods to identify traffic for Cloud Web Security policy.

You can use the following methods of determining the identity of a user or of providing a default identity:

- Identity firewall—When the ASA uses identity firewall with Active Directory (AD), the username and group is retrieved from the AD agent. Users and groups are retrieved when you use them in an ACL in a feature such as an access rule or in your service policy, or by configuring the user identity monitor to download user identity information directly.

  For information about configuring IDFW, see the general operations configuration guide.
- AAA rules—When the ASA performs user authentication using a AAA rule, the username is retrieved from the AAA server or local database. Identity from AAA rules does not include group information. If you configure a default group, these users are associated with that default group. For information about configuring AAA rules, see the legacy feature guide.
- Default username and group—For traffic that does not have an associated user name or group, you can configure an optional default username and group name. These defaults are applied to all users that match a service policy rule for Cloud Web Security.

Authentication Keys

Each ASA must use an authentication key that you obtain from Cloud Web Security. The authentication key lets Cloud Web Security identify the company associated with web requests and ensures that the ASA is associated with a valid customer.

You can use one of two types of authentication keys for your ASA: the company key or the group key.

- **Company authentication key**—You can use a company authentication key on multiple ASAs within the same company. This key simply enables the Cloud Web Security service for your ASAs.
- **Group authentication key**—A Group authentication key is a special key unique to each ASA that performs two functions:
  - Enables the Cloud Web Security service for one ASA.
  - Identifies all traffic from the ASA so you can create ScanCenter policy per ASA.

You generate these keys in ScanCenter (https://scancenter.scansafe.com/portal/admin/login.jsp). For more information, see the Cloud Web Security documentation:

http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html

ScanCenter Policy

In ScanCenter, traffic is matched against policy rules in order until a rule is matched. Cloud Web Security then applies the configured action for the rule, allowing or blocking the traffic, or warning the user. With warnings, the user has the option to continue on to the web site.

You configure the URL filtering policies in ScanCenter, not in the ASA.

However, part of the policy is to whom the policy applies. User traffic can match a policy rule in ScanCenter based on group association: a *directory group* or a *custom group*. Group information is included in the requests redirected from the ASA, so you need to understand what group information you might get from the ASA.

- Directory Groups, page 14-3
- Custom Groups, page 14-3
- How Groups and the Authentication Key Interoperate, page 14-4

Directory Groups

Directory groups define the group to which traffic belongs. When using the identity firewall, the group, if present, is included in the client's HTTP request. If you do not use identity firewall, you can configure a default group for traffic matching an ASA rule for Cloud Web Security inspection.

In ScanCenter, when you configure a directory group in a policy, you must enter the group name exactly.

- Identity firewall group names are sent in the following format.

  *domain-name**group-name*

  Note that on the ASA, the format is *domain-name**group-name*. However, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation when including the group in the redirected HTTP request.

- The default group name is sent in the following format:

  [*domain*\]*group-name*

  On the ASA, you need to configure the optional domain name to be followed by 2 backslashes (\\); however, the ASA modifies the name to use only one backslash (\) to conform to typical ScanCenter notation. For example, if you specify "Cisco\\Boulder1," the ASA modifies the group name to be "Cisco\Boulder1" with only one backslash (\) when sending the group name to Cloud Web Security.

Custom Groups

Custom groups are defined using one or more of the following criteria:

- ScanCenter Group authentication key—You can generate a Group authentication key for a custom group. Then, if you identify this group key when you configure the ASA, all traffic from the ASA is tagged with the Group key.
- Source IP address—You can identify source IP addresses in the custom group. Note that the ASA service policy is based on source IP address, so you might want to configure any IP address-based policy on the ASA instead.
- Username—You can identify usernames in the custom group.
  - Identity firewall usernames are sent in the following format:

    *domain-name**username*
  - AAA usernames, when using RADIUS or TACACS+, are sent in the following format:

    LOCAL*username*
  - AAA usernames, when using LDAP, are sent in the following format:

    *domain-name**username*

– For the default username, it is sent in the following format:

  [*domain-name*\]*username*

  For example, if you configure the default username to be “Guest,” then the ASA sends “Guest.” If you configure the default username to be “Cisco\Guest,” then the ASA sends “Cisco\Guest.”

How Groups and the Authentication Key Interoperate

Unless you need the per-ASA policy that a custom group plus group key provides, you will likely use a company key. Note that not all custom groups are associated with a group key. You can use non-keyed custom groups to identify IP addresses or usernames, and use them in your policy along with rules that use directory groups.

Even if you do want per-ASA policy and are using a group key, you can also use the matching capability provided by directory groups and non-keyed custom groups. In this case, you might want an ASA-based policy, with some exceptions based on group membership, IP address, or username. For example, if you want to exempt users in the America\Management group across all ASAs:

1. Add a directory group for America\Management.
2. Add an exempt rule for this group.
3. Add rules for each custom group plus group key after the exempt rule to apply policy per-ASA.
4. Traffic from users in America\Management will match the exempt rule, while all other traffic will match the rule for the ASA from which it originated.

Many combinations of keys, groups, and policy rules are possible.

Failover from Primary to Backup Proxy Server

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 minutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

You can also choose how the ASA handles web traffic when it cannot reach either the primary or backup Cloud Web Security proxy server. It can block or allow all web traffic. By default, it blocks web traffic.

Licensing Requirements for Cisco Cloud Web Security

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Strong Encryption (3DES/AES) License to encrypt traffic between the security appliance and the Cloud Web Security server.

On the Cloud Web Security side, you must purchase a Cisco Cloud Web Security license and identify the number of users that the ASA handles. Then log into ScanCenter and generate your authentication keys.

Guidelines for Cloud Web Security

Context Mode Guidelines

Supported in single and multiple context modes.

In multiple context mode, the server configuration is allowed only in the system context, and the service policy rule configuration is allowed only in the security contexts.

Each context can have its own authentication key, if desired.

Firewall Mode Guidelines

Supported in routed firewall mode only. Does not support transparent firewall mode.

IPv6 Guidelines

Does not support IPv6. Cloud Web Security currently supports only IPv4 addresses. If you use IPv6 internally, use NAT 64 to translate IPv6 addresses to IPv4 for any IPv6 flows that need to be sent to Cloud Web Security.

Additional Guidelines

- Cloud Web Security is not supported with ASA clustering.
- You cannot use Cloud Web Security on the same traffic you redirect to a module that can also perform URL filtering, such as ASA CX and ASA FirePOWER. The traffic is sent to the modules only, not to the Cloud Web Security servers.
- Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security.
- When an interface to the Cloud Web Security proxy servers goes down, output from the **show scansafe server** command shows both servers up for approximately 15-25 minutes. This condition may occur because the polling mechanism is based on the active connection, and because that interface is down, it shows zero connection, and it takes the longest poll time approach.
- Cloud Web Security inspection is compatible with HTTP inspection for the same traffic.
- Cloud Web Security is not supported with extended PAT or any application that can potentially use the same source port and IP address for separate connections. For example, if two different connections (targeted to separate servers) use extended PAT, the ASA might reuse the same source IP and source port for both connection translations because they are differentiated by the separate destinations. When the ASA redirects these connections to the Cloud Web Security server, it replaces the destination with the Cloud Web Security server IP address and port (8080 by default). As a result, both connections now appear to belong to the same flow (same source IP/port and destination IP/port), and return traffic cannot be untranslated properly.
- The default inspection traffic class does not include the default ports for the Cloud Web Security inspection (80 and 443).

Configure Cisco Cloud Web Security

Before you configure Cloud Web Security, obtain a license and the addresses of the proxy servers you will use. Also, generate your authentication keys. Learn more about at Cloud Web Security http://www.cisco.com/go/cloudwebsecurity.

Use the following process to configure the ASA to redirect web traffic to Cloud Web Security.

Before You Begin

If you want to send user identity information to Cloud Web Security, configure one of the following on the ASA:

- Identity firewall (username and group).
- AAA rules (username only)—See the legacy feature guide.

If you want to use fully-qualified domain names (FQDN), such as www.example.com, you must configure a DNS server for the ASA.

Procedure

Step 1 Configure Communications with the Cloud Web Security Proxy Server, page 14-6.

Step 2 (Optional.) Identify Whitelisted Traffic, page 14-8.

Step 3 Configure a Service Policy to Send Traffic to Cloud Web Security, page 14-9.

Step 4 (Optional.) Configure the User Identity Monitor, page 14-13

Step 5 Configure the Cloud Web Security Policy, page 14-14.

Configure Communications with the Cloud Web Security Proxy Server

You must identify the Cloud Web Security proxy servers so that user web requests can be redirected properly.

In multiple context mode, you must configure the proxy servers in the system context, then enable Cloud Web Security per context. Thus, you can use the service in some contexts but not in others.

Before You Begin

- You must configure a DNS server for the ASA to use fully-qualified domain names for the proxy servers.
- (Multiple context mode.) You must configure a route pointing to the Cloud Web Security proxy servers in both the system context and the specific contexts. This ensures that the Cloud Web Security proxy servers do not become unreachable in the Active/Active failover scenario.

Procedure

Step 1 Enter ScanSafe general-options configuration mode. In multiple context mode, do this in the system context.

```
scansafe general-options
```

Example

```
hostname(config)# scansafe general-options
```

Step 2 Configure the primary and secondary Cloud Web Security proxy servers.

```
server primary {ip ip_address | fqdn fqdn} [port port]
server backup {ip ip_address | fqdn fqdn} [port port]
```

Example

```
hostname(cfg-scansafe)# server primary ip 192.168.43.10
hostname(cfg-scansafe)# server backup fqdn server.example.com
```

When you subscribe to the Cisco Cloud Web Security service, you are assigned primary and backup Cloud Web Security proxy servers. Enter their IP addresses (**ip**), or fully-qualified domain names (**fqdn**), on these commands.

By default, the Cloud Web Security proxy server uses port 8080 for both HTTP and HTTPS traffic; do not change this value unless directed to do so.

Step 3 (Optional.) Configure the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable.

```
retry-count value
```

Example

```
hostname(cfg-scansafe)# retry-count 2
```

Polls are performed every 30 seconds. Valid values are from 2 to 100, and the default is 5.

Step 4 Configure the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.

```
license hex_key
```

Example

```
hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3
```

The authentication key is a 16-byte hexidecimal number. It can be a company or group key.

Step 5 (Multiple context mode only.) Switch to each context where you want to use the service and enable it.

```
scansafe [license hex_key]
```

Example

```
hostname(config)# changeto context one
hostname/one(config)# scansafe
```

You can optionally enter a separate authentication key for each context. If you do not include an authentication key, the one configured for the system context is used.

Examples

The following example configures a primary and backup server:

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

The following sample configuration enables Cloud Web Security in context one with the default license and in context two with the license key override:

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

Identify Whitelisted Traffic

If you use identity firewall or AAA rules, you can configure the ASA so that web traffic from specific users or groups that otherwise match the service policy rule is not redirected to the Cloud Web Security proxy server for scanning. This process is called “whitelisting” traffic.

You configure the whitelist in a ScanSafe inspection class map. You can use usernames and group names derived from both identity firewall and AAA rules. You cannot whitelist based on IP address or on destination URL.

When you configure your Cloud Web Security service policy rule, you refer to the class map in your policy. Although you can achieve the same results of exempting traffic based on user or group when you configure the traffic matching criteria (with ACLs) in the service policy rule, you might find it more straightforward to use a whitelist instead.

Procedure

Step 1 Create the class map.

```
hostname(config)# class-map type inspect scansafe [match-all | match-any] class_map_name
hostname(config-cmap)#
```

Where the *class_map_name* is the name of the class map. The **match-all** keyword is the default, and specifies that traffic must match all criteria to match the class map. The match-any keyword specifies that the traffic matches the class map if it matches at least one **match** statement. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

Example

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
```

Step 2 Specify the whitelisted users and groups.

```
match [not] {[user username] [group groupname]}
```

The **match** keyword specifies a user or group to whitelist, or both.

The **match not** keyword specifies that the user or group should be filtered using Cloud Web Security. For example, if you whitelist the group "cisco," but you want to scan traffic from users "johncrichton" and "aerynsun," which are members of that group, you can specify **match not** for those users. Repeat this command to add as many users and groups as needed.

Example

The following example whitelists the same users and groups for the HTTP and HTTPS inspection policy maps:

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

Configure a Service Policy to Send Traffic to Cloud Web Security

Your service policy consists of multiple service policy rules, applied globally, or applied to each interface. Each service policy rule can either send traffic to Cloud Web Security (Match) or exempt traffic from Cloud Web Security (Do Not Match).

Create rules for traffic destined for the Internet. The order of these rules is important. When the ASA decides whether to forward or exempt a packet, the ASA tests the packet with each rule in the order in which the rules are listed. After a match is found, no more rules are checked. For example, if you create a rule at the beginning of a policy that explicitly Matches all traffic, no further statements are ever checked.

Before You Begin

If you need to use a whitelist to exempt some traffic from being sent to Cloud Web Security, first create the whitelist so you can refer to it in your service policy rule.

Procedure

Step 1 Create the ScanSafe inspection policy maps. You need to define separate maps for HTTP and HTTPS.

a. Create the ScanSafe inspection policy map.

```
hostname(config)# policy-map type inspect scansafe policy_map_name
```

```
hostname(config-pmap)#
```

Where the *policy_map_name* is the name of the policy map. The CLI enters policy-map configuration mode.

b. Enter parameters configuration mode.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

c. Set one or more parameters. You can set the following options; use the **no** form of the command to disable the option:

- {**http** | **https**}—The service type for this map. You can only specify one service type per map, so you need separate maps for HTTP and HTTPS.
- **default** {[**user** *username*] [**group** *groupname*]}—(Optional.) The default user or group name, or both. If the ASA cannot determine the identity of the user coming into the ASA, then the default user and group is included in the HTTP request sent to Cloud Web Security. You can define policies in ScanCenter for this user or group name.

d. (Optional.) If you defined a whitelist, identify the class and use the **whitelist** command to mark it as a whitelist.

```
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

e. Repeat the process to create an inspection policy map for the other protocol, HTTP or HTTPS.

Step 2 Define the classes for the traffic you want to redirect to Cloud Web Security.

ACL matching is the most flexible way to define the class. However, if you want to send all HTTP/HTTPS traffic, you could instead use a port match in the class (**match port tcp 80** and **match port tcp 443**). The following procedure describes an ACL match.

a. Create ACLs (**access-list extended** command) to identify the traffic you want to send to Cloud Web Security. You must create separate ACLs for HTTP and HTTPS traffic. Because Cloud Web Security works on HTTP/HTTPS traffic only, any other traffic defined in the ACL is ignored.

A **permit** ACE sends matching traffic to Cloud Web Security. A **deny** ACE exempts traffic from the service policy rule, so it is not sent to Cloud Web Security. Use **tcp** for the protocol, and identify the port (80 for HTTP, 443 for HTTPS).

When creating your ACLs, consider how you can match appropriate traffic that is destined for the Internet, but not match traffic that is destined for other internal networks. For example, to prevent inside traffic from being sent to Cloud Web Security when the destination is an internal server on the DMZ, be sure to add a deny ACE to the ACL that exempts traffic to the DMZ.

FQDN network objects might be useful in exempting traffic to specific servers. You can also use identity firewall user arguments and Cisco Trustsec security groups to help identify traffic. Note that Trustsec security group information is not sent to Cloud Web Security; you cannot define policy based on security group.

Create as many ACLs as needed for your policy. You can apply redirection to any number of traffic classes.

The following example shows how to exempt HTTP traffic to two servers, but include the remaining traffic. You would create a duplicate ACL for HTTPS traffic, where you simply change the port to 443.

```
hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com

hostname(config)# object network cisco2
```

```
hostname(config-object-network)# fqdn tools.cisco.com

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
```

b. Create a traffic class for each ACL you defined.

```
hostname(config)# class-map class_name
hostname(config-cmap)# match access-list acl_name
```

Example

```
hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS
```

Step 3 Create or edit the policy map to redirect the traffic to Cloud Web Security.

a. Add or edit a policy map that sets the actions to take with the class map traffic. In the default configuration, the global_policy policy map is assigned globally to all interfaces. If you want to edit the global_policy, enter global_policy as the policy name. You can only apply one policy to each interface or globally.

```
policy-map name
```

Example:

```
hostname(config)# policy-map global_policy
```

b. Identify one of the traffic class maps you created for Cloud Web Security inspection.

```
class name
```

Example:

```
hostname(config-pmap)# class cws_class1
```

c. Configure ScanSafe inspection for the class.

```
inspect scansafe scansafe_policy_map [fail-open | fail-close]
```

Where:

- *scansafe_policy_map* is the ScanSafe inspection policy map. Ensure that you match the protocols in the class and policy maps (both HTTP or HTTPS).
- Specify **fail-open** to allow traffic to pass through the ASA if the Cloud Web Security servers are unavailable.
- Specify **fail-close** to drop all traffic if the Cloud Web Security servers are unavailable. **fail-close** is the default.

Example:

```
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
```

Note If you are editing the default global policy (or any in-use policy) to use a different ScanSafe inspection policy map, you must remove the ScanSafe inspection with the **no inspect scansafe** command, and then re-add it with the new inspection policy map name.

d. Add the class for the other protocol and enable inspection. If you have additional classes, add them also.

```
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
```

Step 4 If you are editing an existing service policy (such as the default global policy called global_policy), you are done. Otherwise, activate the policy map on one or more interfaces.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

Example:

```
hostname(config)# service-policy global_policy global
```

The **global** keyword applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

Examples

The following example configures two classes: one for HTTP and one for HTTPS. Each ACL exempts traffic to www.cisco.com and to tools.cisco.com, and to the DMZ network, for both HTTP and HTTPS. All other traffic is sent to Cloud Web Security, except for traffic from several whitelisted users and groups. The policy is then applied to the inside interface.

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
```

```
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
hostname(config)# service-policy cws_policy inside
```

Configure the User Identity Monitor

When you use identity firewall, the ASA only downloads user identity information from the AD server for users and groups included in active ACLs. The ACL must be used in a feature such as an access rule, AAA rule, service policy rule, or other feature to be considered active.

For example, although you can configure your Cloud Web Security service policy rule to use an ACL with users and groups, thus activating any relevant groups, it is not required. You could use an ACL based entirely on IP addresses.

Because Cloud Web Security can base its ScanCenter policy on user identity, you might need to download groups that are not part of an active ACL to get full identity firewall coverage for all your users. The user identity monitor lets you download group information directly from the AD agent.

Note The ASA can only monitor a maximum of 512 groups, including those configured for the user identity monitor and those monitored through active ACLs.

Procedure

Step 1 Identify the groups that you want to use in ScanCenter policies that are not already used in active ACLs. If necessary, create local user group objects.

Step 2 Download the group information from the AD agent.

user-identity monitor {**user-group** [*domain-name*****]*group-name* | **object-group-user** *object-group-name*}

```
hostname(config)# user-identity monitor user-group CISCO\\Engineering
```

Where:

- **user-group**—Specifies a group name defined in the AD server.
- **object-group-user**—The name of a local object created by the **object-group user** command. This group can include multiple groups.

Configure the Cloud Web Security Policy

After you configure the ASA service policy rules, launch the ScanCenter Portal to configure Web content scanning, filtering, malware protection services, and reports.

Go to: https://scancenter.scansafe.com/portal/admin/login.jsp.

For more information, see the Cisco ScanSafe Cloud Web Security Configuration Guides:

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Monitoring Cloud Web Security

To monitor Cloud Web Security, use the following commands:

- **show scansafe server**

  Shows the status of the server, whether it is the currently active server, the backup server, or unreachable.

```
hostname# show scansafe server
hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
hostname# Backup: proxy137.scansafe.net (80.254.152.99)
```

- **show scansafe statistics**

  Shows information about Cloud Web Security activity, such as the number of connections redirected to the proxy server, the number of current connections being redirected, and the number of white listed connections:

```
hostname# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

- **show service policy inspect scansafe**

  Shows the number of connections that are redirected or white listed by a particular policy.

```
hostname(config)# show service-policy inspect scansafe
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
  Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-open"
config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
```

```
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

- **show conn scansafe**

  Shows all Cloud Web Security connections, as noted by the capitol Z flag.

You can determine if a user's traffic is being redirected to the proxy servers by accessing the following URL from the client machine. The page will show a message indicating whether the user is currently using the service.

http://Whoami.scansafe.net

Examples for Cisco Cloud Web Security

Following are some examples for configuring Cloud Web Security.

- Cloud Web Security Example with Identity Firewall, page 14-15
- Active Directory Integration Example for Identity Firewall, page 14-17

Cloud Web Security Example with Identity Firewall

The following example shows a complete configuration for Cisco Cloud Web Security in single context mode, including the optional configuration for identity firewall.

Step 1 Configure Cloud Web Security on the ASA.

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Step 2 Configure identity firewall settings.

Because groups are a key feature of ScanCenter policies, you should consider enabling the identity firewall if you are not already using it. However, identity firewall is optional. The following example shows how to define the Active Directory (AD) server, the AD agent, configure identity firewall settings, and enable the user identity monitor for a few groups.

```
aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
 server-port 389
 ldap-base-dn DC=ASASCANLAB,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
 server-type microsoft
aaa-server adagent protocol radius
 ad-agent-mode
aaa-server adagent (inside) host 192.168.116.220
 key *****
user-identity domain ASASCANLAB aaa-server AD
user-identity default-domain ASASCANLAB
user-identity action netbios-response-fail remove-user-ip
user-identity poll-import-user-group-timer hours 1
user-identity ad-agent aaa-server adagent
user-identity user-not-found enable
user-identity monitor user-group ASASCANLAB\\GROUP1
```

```
user-identity monitor user-group ASASCANLAB\\GROUPNAME
```

Step 3 (Optional) Configure a whitelist.

If there are specific users or groups you would like to exempt from Cloud Web Security filtering, you can create a whitelist.

```
class-map type inspect scansafe match-any whiteListCmap
 match user LOCAL\user1
```

Step 4 Configure ACLs.

We recommend that you split the traffic by creating separate HTTP and HTTPS class maps so that you know how many HTTP and HTTPS packets have gone through.

Then, if you need to troubleshoot you can run debug commands to distinguish how many packets have traversed each class map and find out if you are pushing through more HTTP or HTTPS traffic:

```
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

Step 5 Configure class maps.

```
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

hostname(config)# class-map cmap-https
hostname(config-cmap)# match access-list https
```

Step 6 Configure inspection policy maps.

```
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist

hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstraffic
hostname(config-pmap-p)# https
hostname(config-pmap-p)# class whiteListCmap
hostname(config-pmap-p)# whitelist
```

Step 7 Configure policy maps.

The following example creates unique policy maps for Cloud Web Security traffic.

```
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

Alternatively, you can add the classes to the default global_policy to have redirection enabled for all interfaces. Ensure that you add the classes to global_policy rather than applying a new policy map globally, or you will remove the default protocol inspections that are part of the default global policy.

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

Step 8 Configure service policy.

If you created a separate policy map for Cloud Web Security, the following example shows how to apply it to an interface. If you instead added the classes to the global_policy map, you are finished; you do not need to enter the service-policy command.

```
hostname(config)# service-policy pmap-webtraffic interface inside
```

Active Directory Integration Example for Identity Firewall

The following is an end-to-end example configuration for Active Directory integration. This configuration enables the identity firewall.

Procedure

Step 1 Configure the Active Directory Server Using LDAP.

The following example shows how to configure the Active Directory server on your ASA using LDAP:

```
hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn
cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1
```

Step 2 Configure the Active Directory Agent Using RADIUS.

The following example shows how to configure the Active Directory Agent on your ASA using RADIUS:

```
hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent
```

Step 3 (On the AD Agent server.) Create the ASA as a Client on the AD Agent Server.

The following example shows how to create the ASA as a client on the Active Directory agent server:

```
c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123
```

Step 4 (On the AD Agent server.) Create a Link Between the AD Agent and DCs.

The following example shows how to create a link between the Active Directory Agent and all DCs for which you want to monitor logon/logoff events:

```
c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC -domain
W2K3DC.asascanlab.local -user administrator -password Password1
c:\IBF\CLI\adacfg.exe dc list
```

Running the last command should show the status as “UP.”

For the AD_Agent to monitor logon/logoff events, you need to ensure that these are logged on all DCs that are actively being monitored. To do this, choose:

Start > Administrative Tools > Domain Controller Security Policy

Local policies > Audit Policy > Audit account logon events (success and failure)

Step 5 (Back on the ASA.) Test the AD Agent.

The following example shows how to configure the test Active Directory Agent so that it can communicate with the ASA:

```
hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)
INFO: Ad-agent Successful
```

See also the following command: **show user-identity ad-agent**.

Step 6 Configure the Identity Options on the ASA.

The following example shows how to configure the identity options on the ASA:

```
hostname(config)# user-identity domain ASASCANLAB aaa-server AD
hostname(config)# user-identity default-domain ASASCANLAB
```

Step 7 Configure the User Identity Options and Enabling Granular Reporting.

The following example shows how to configure the user identity options that send user credentials to the ASA and enable granular user reporting from the proxy server:

```
hostname(config)# user-identity inactive-user-timer minutes 60
hostname(config)# user-identity action netbios-response-fail remove-user-ip
hostname(config)# user-identity user-not-found enable
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download
```

There are two download modes with Identify Firewall: Full download and On-demand.

- Full download—Whenever a user logs into the network, the IDFW tells the ASA the User identity immediately (recommended on the ASA 5512-X and above).
- On-demand—Whenever a user logs into the network, the ASA requests the user identity from AD.

If you are using more than one domain, then enter the following command:

```
hostname(config)# user-identity domain OTHERDOMAINNAME
```

Step 8 Monitor the Active Directory Groups.

The following example shows how to configure Active Directory groups to be monitored:

```
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME3
```

Remember to save your configuration once the above is completed.

Step 9 Download the Entire Active-User Database from the Active Directory Server.

The following command updates the specified import user group database by querying the Active Directory server immediately without waiting for the expiration of poll-import-user-group-timer:

```
hostname(config)# user-identity update import-user
```

Step 10 Download the Database from the AD Agent.

The following example shows how to manually start the download of the database from the Active Directory Agent if you think the user database is out of sync with Active Directory:

```
hostname(config)# user-identity update active-user-database
```

Step 11 Show a List of Active Users.

```
hostname# show user-identity user active list detail
```

History for Cisco Cloud Web Security

Feature Name	Platform Releases	Feature Information
Cloud Web Security	9.0(1)	This feature was introduced. Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity. We introduced or modified the following commands: **class-map type inspect scansafe**, **default user group**, **http**[**s**] (parameters), **inspect scansafe**, **license**, **match user group**, **policy-map type inspect scansafe**, **retry-count**, **scansafe**, **scansafe general-options**, **server** {**primary** | **backup**}, **show conn scansafe**, **show scansafe server**, **show scansafe statistics**, **user-identity monitor**, **whitelist**.