

dn – dz

- dnscrypt, on page 3
- dns domain-lookup, on page 5
- dns expire-entry-timer, on page 7
- dns-group, on page 9
- dns-group-map, on page 11
- dns-guard, on page 13
- dns-id, on page 14
- dns name-server, on page 16
- dns poll-timer, on page 18
- dns-server (group-policy), on page 19
- dns-server (ipv6 dhcp pool), on page 21
- dns server-group, on page 24
- dns-to-domain, on page 26
- dns trusted-source, on page 28
- dns update, on page 30
- domain, on page 32
- domain-name (dns server-group), on page 34
- domain-name (global), on page 35
- domain-name (ipv6 dhcp pool), on page 36
- domain-password, on page 39
- downgrade, on page 43
- download-max-size, on page 45
- drop, on page 47
- drop-connection, on page 49
- dtls port, on page 51
- duplex, on page 52
- dynamic-access-policy-config, on page 54
- dynamic-access-policy-record, on page 56
- dynamic-authorization, on page 58
- dynamic-filter ambiguous-is-black, on page 60
- dynamic-filter blacklist, on page 63
- dynamic-filter database fetch, on page 66
- dynamic-filter database find, on page 68

- dynamic-filter database purge, on page 71
- dynamic-filter drop blacklist, on page 73
- dynamic-filter enable, on page 76
- dynamic-filter updater-client enable, on page 79
- dynamic-filter use-database, on page 82
- dynamic-filter whitelist, on page 85

dnscrypt

To enable DNScrypt to encrypt connections between the device and Cisco Umbrella, use the **dnscrypt** command in DNS inspection policy map parameters configuration mode. To disable DNScrypt, use the **no** form of this command.

dnscrypt
no dnscrypt

Syntax Description

This command has no arguments or keywords.

Command Default

DNScrypt is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

Use this command when configuring a DNS inspection policy map.

Enabling DNScrypt starts the key-exchange thread with the Umbrella resolver. The key-exchange thread performs the handshake with the resolver every hour and updates the device with a new secret key.

Because DNScrypt uses UDP/443, you must ensure that the class map used for DNS inspection includes that port. Note that the default inspection class already includes UDP/443 for DNS inspection.

Examples

The following example enables Umbrella using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection. The global DNS inspection already applies to UDP/443.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
umbrella-global	Configures the Cisco Umbrella global parameters.
umbrella	Enables the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella.

dns domain-lookup

To enable the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands, use the **dns domain-lookup** command in global configuration mode. To disable DNS requests, use the **no** form of this command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns domain-lookup *interface_name*
no dns domain-lookup *interface_name*

Syntax Description

interface_name	Specifies the name of the configured interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Make sure to enable DNS lookup on all interfaces that will be used to access DNS servers.

After you enable DNS lookup, specify DNS servers for the default server group using the **dns server-group DefaultDNS** server group command, and then the **name-server** command. You can change the default server group using the **dns-group** command.

Other server groups can be associated with specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. Other DNS server groups can be configured for VPN tunnel groups. See the **tunnel-group** command for more information.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example enable the ASA to send DNS requests to a DNS server to perform a name lookup for the management, inside, and dmz interfaces.

```
ciscoasa(config)# dns domain-lookup management
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup dmz
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 management
ciscoasa(config-dns-server-group)# name-server 10.10.1.1 10.20.2.2
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns expire-entry-timer

To remove the IP address of a resolved FQDN after its TTL expires, use the **dns expire-entry-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

dns expire-entry-timer minutes *minutes*
no dns expire-entry-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer time in minutes. Valid values range from 1 to 65535 minutes.

Command Default

By default, the DNS expire-entry-timer value is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The command specifies the time to remove the IP address of a resolved FQDN after its TTL expires. When the IP address is removed, the ASA recompiles the tmatch lookup table.

Specifying this command is only effective when the associated network object for the DNS is activated.

The default DNS expire-entry-timer value is 1 minute, which means that IP addresses are removed 1 minute after the TTL of the DNS entry expires.

Note The default setting might result in frequent recompilation of the tmatch lookup table when the resolved TTL of common FQDN hosts, such as www.sample.com, is a short time period. You can specify a long DNS expire-entry timer value to reduce the frequency of recompilation of the tmatch lookup table while maintaining security.

Examples

The following example removes resolved entries after 240 minutes:

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns-group

To specify the default DNS group, use the **dns-group** command in global configuration mode. To specify the DNS server group per tunnel group, use the **dns-group** command in tunnel-group webvpn-attributes configuration mode. To restore the default DNS group, use the **no** form of this command.

dns-group*name*
no dns-group

Syntax Description

name	Specifies the name of the default DNS server group. The default group cannot have any associated domains in the **dns-group-map**.

Command Default

The default value is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

You configure the default DNS group using the **dns server-group** command.

Examples

The following example shows a customization command that specifies the use of the DNS group named “dnsgroup1”:

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel group attributes.

dns-group-map

To map DNS server groups to specific domains, use the **dns-group-map** command in global configuration mode. To remove the DNS group map, use the **no** form of this command.

dns-group-map
no dns-group-map

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	Added this command.

Usage Guidelines

After you enter the **dns-group-map** command, add server-group-to-domain mappings using the **dns-to-domain** command. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface.

Examples

The following example configures three mappings:

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.

Command	Description
dns-to-domain	Maps a DNS server group to a domain.
name-server	Adds a DNS server to a group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns-guard

To enable the DNS guard function, which enforces one DNS response per query, use the **dns-guard** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

dns-guard
no dns-guard

Syntax Description

This command has no arguments or keywords.

Command Default

DNS guard is enabled by default. This feature can be enabled when the **inspect dns** command is configured even if a **policy-map type inspect dns** command is not defined. To disable, the **no dns-guard** command must explicitly be stated in the policy map configuration. If the **inspect dns** command is not configured, the behavior is determined by the global dns-guard command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The identification field in the DNS header is used to match the DNS response with the DNS header. One response per query is allowed through the ASA.

Examples

The following example shows how to enable DNS guard in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# dns-guard
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

dns-id

To configure a dns-id in a reference-identity object, use the **dns-id** command in ca-reference-identity mode. To delete a dns-id, use the **no** form of this command. You can access the *ca-reference-identity* mode by first entering the **crypto ca reference-identity** command to configure a reference-identity object..

dns-id*value*
no dns-id *value*

Syntax Description

value	Value of each reference-id.
dns-id	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca-reference-identity	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

The reference identifiers **cn-id** and **dns-id** MAY NOT contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
crypto ca reference-identity	Configures a reference identity object.
cn-id	Configures a Common Name Identifier in the reference-identity object.

Command	Description
srv-id	Configures a SRV-ID identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

dns name-server

To configure a DNS server for the *default* DNS server group, use the **dns name-server** command in global configuration mode. To remove the configuration, use the **no** form of this command. This command is equivalent to the **name-server** command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]
no dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

Syntax Description

ip_address Specifies the IPv4 or IPv6 address of the DNS server. You can specify up to 6 addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	This command was changed to add the DNS servers under the **dns server-group DefaultDNS** server group.
9.0(1)	Support for IPv6 addresses was added.

Usage Guidelines

To enable DNS lookup for an interface, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used on that interface.

This command adds servers to the default DNS server group. By default, the default group is called **DefaultDNS**. You can change the default group using the **dns-group** command. See the following resulting configuration:

```
ciscoasa(config)# dns name-server 10.1.1.1
ciscoasa(config)# show running-config dns
```

```
dns server-group DefaultDNS
name-server ip_address
```

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example configures a DNS server with an IPv6 address:

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns poll-timer

To specify the timer during which the ASA queries the DNS server to resolve fully qualified domain names (FQDN) that are defined in a network object group, use the **dns poll-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

dns poll-timer minutes *minutes*
no dns poll-timer minutes *minutes*

Syntax Description

minutes *minutes*	Specifies the timer in minutes. Valid values are from 1 to 65535 minutes.

Command Default

By default, the DNS timer is 240 minutes or 4 hours.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command specifies the timer during which the ASA queries the DNS server to resolve the FQDN that was defined in a network object group. A FQDN is resolved periodically when the poll DNS timer has expired or when the TTL of the resolved IP entry has expired, whichever comes first.

This command has effect only when at least one network object group has been activated.

Examples

The following example sets the DNS poll timer to 240 minutes:

```
ciscoasa(config)# dns poll-timer minutes 240
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.

dns-server (group-policy)

To set the IP address of the primary and secondary DNS servers, use the **dns-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

dns-server { **value** *ip_address* [*ip_address*] | **none** }
no dns-server

Syntax Description

none	Sets the **dns-server** command to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary DNS servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command allows inheritance of a DNS server from another group policy. To prevent inheriting a server, use the **dns-server none** command.

Each time you issue the **dns-server** command, you overwrite the existing setting. For example, if you configure DNS server x.x.x.x and then configure DNS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole DNS server. The same holds true for multiple servers. To add a DNS server rather than overwrite previously configured servers, include the IP addresses of all DNS servers when you enter this command.

Examples

The following example shows how to configure DNS servers with the IP addresses 10.10.10.15 and 10.10.10.45 for the group policy named FirstGroup.

```
ciscoasa
(config)#
group-policy FirstGroup attributes
ciscoasa
```

```
(config-group-policy)#
 dns-server value 10.10.10.15 10.10.10.45
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
show running-config dns server-group	Shows the current running DNS server group configuration.

dns-server (ipv6 dhcp pool)

To provide the DNS server IP address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **dns-server** command in ipv6 dhcp pool configuration mode. To remove the DNS server, use the **no** form of this command.

dns-server*dns_ipv6_address*
no dns-server *dns_ipv6_address*

Syntax Description

dns_ipv6_address	Specifies the DNS server IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the DNS server, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
```

```
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.

Command	Description
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

dns server-group

To create and configure a group of DNS servers, use the **dns server-group** command in global configuration mode. To remove a particular DNS server group, use the **no** form of this command.

Note The ASA has limited support for using the DNS server, depending on the feature. For example, most commands require you to enter an IP address and can only use a name when you manually configure the **name** command to associate a name with an IP address and enable use of the names using the **names** command.

dns server-group *name*
nodnsserver-group

Syntax Description

name Specifies the name of the DNS server group. The default group name used for ASA lookups is **DefaultDNS**.

Command Default

The default active server group for the ASA is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

To enable DNS lookup, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used.

The ASA uses the **dns server-group DefaultDNS** server group for outgoing requests. You can change the active server group using the **dns-group** command. Other DNS server groups can be configured for VPN tunnel groups or other purposes. See the **tunnel-group** command for more information.

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database; and Cisco Smart Software Licensing needs DNS to resolve the License Authority address. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names. You also must configure DNS servers to use fully qualified domain names (FQDN) network objects in access rules.

Examples

The following example configures a DNS server group named “DefaultDNS”:

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
expire-entry-timer	Only available for DefaultDNS. Sets the time added to the TTL value returned by the DNS server to calculate the delete timer.
poll-timer	Only available for DefaultDNS. Specifies the timer to periodically resolve an FQDN defined in a network object.
retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
show running-config dns server-group	Shows the current running DNS server group configuration.
timeout	Specifies the amount of time to wait before trying the next DNS server.

dns-to-domain

To map a DNS server groups to a specific domain, use the **dns-to-domain** command in dns-group-map configuration mode. To remove the mapping, use the **no** form of this command.

dns-to-domain *dns_group_name domain*
no dns-to-domain *dns_group_name domain*

Syntax Description

dns_group_name	Specifies the DNS group name from the **dns server-group** command that you want to use for the associated domain. Do not map any domains to the group you want to use for the default (for example, DefaultDNS).
domain	Specifies the domain for which you want to use the associated DNS server group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dns-group-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	Added this command.

Usage Guidelines

By default, there is a default DNS server group called DefaultDNS. You can create multiple DNS server groups: one group is the default, while other groups can be associated with specific domains by using the **dns-group-map** and **dns-to-domain** commands. A DNS request that matches a domain associated with a DNS server group will use that group. You can create up to 30 mappings.

For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface.

Examples

The following example configures three mappings:

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
```

```
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns server-group mode, in which you can configure a DNS servers.
dns-group-map	Maps DNS server groups to domains.
name-server	Adds a DNS server to a group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

dns trusted-source

To define the DNS servers that can be trusted to resolve domain names in a network-service object, use the **dns trusted-source** command in global configuration mode. To remove a type of DNS server from the trusted list, use the **no** form of the command.

dns trusted-source { **configured-servers** | **dhcp-client** | **dhcp-pools** | **dhcp-relay** | *ip_list* }

Syntax Description

configured-servers	Specifies that servers configured in DNS server groups should be trusted. A configured server is any server specified in DNS groups or name-server commands.
dhcp-client	Specifies that the servers that are learned by snooping messages between a DHCP client and DHCP server are considered trusted DNS servers. This option applies when you configure the **dhcpd auto_config** command to configure DHCP servers on inside interfaces using the information obtained from device interfaces that use DHCP client to obtain an IP address.
dhcp-pools	Specifies that the DNS servers that are configured in the DHCP pools for clients that obtain addresses through DHCP servers running on the device interfaces should be trusted. These are the servers that are configured on the **dhcpd dns** command, and thus are IPv4 only.
dhcp-relay	Specifies that the servers that are learned by snooping DHCP relay messages between a DHCP client and DHCP server are considered trusted DNS servers.
ip_list	A space separated list of the IP addresses of DNS servers that should be trusted. You can list up to 12 IPv4 and IPv6 addresses. Specify **any** to cover all DNS servers. Use the **no** form of the command to remove a server.

Command Default

By default, all configured and learned DNS servers are trusted (that is, all of these options). You need to change this only if you want to limit the trusted list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Usage Guidelines

If you configure domain names in network-service objects, the system snoops DNS request/response traffic to gather IP addresses for DNS domain names and caches the results. Any DNS request/response can be snooped.

The records snooped are A, AAAA, and MX. The time-to-live (TTL) of each resolved name is honored within limits: the minimum TTL is 2 minutes, the maximum is 24 hours. This ensures that the cache does not become stale.

For security reasons, you can limit the scope of DNS snooping by defining which DNS servers should be trusted. Any DNS traffic to non-trusted DNS servers is ignored and not used to obtain mappings for network-service objects. By default, all configured and learned DNS servers are trusted; you need to change this only if you want to limit the trusted list.

Example

The following example explicitly trusts the DNS servers at 10.100.10.1 and 10.100.10.2.

```
ciscoasa(config)# dns trusted-source 10.100.10.1 10.100.10.2
```

The following example removes DNS relay servers from the trusted server configuration.

```
ciscoasa(config)# no dns trusted-source dhcp-relay
```

Related Commands

Command	Description
show dns trusted-source	Shows the trusted DNS configuration.

dns update

To start DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer, use the **dns update** command in privileged EXEC mode.

dns update [**host** *fqdn_name*] [**timeout seconds** *seconds*]

Syntax Description

host *fqdn_name*	Specifies the fully qualified domain name of the host on which to run DNS updates.
timeout seconds *seconds*	Specifies the timeout in seconds.

Command Default

By default, the timeout is 30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command immediately starts a DNS lookup to resolve the designated hostnames without waiting for the expiration of the DNS poll timer. When you run DNS update without specifying an option, all activated host groups and FQDN hosts are selected for DNS lookup. When the command finishes running, the ASA displays [Done] at the command prompt and generates a syslog message.

When the update operation starts, a starting update log is created. When the update operation finishes or is aborted after the timer has expired, another syslog message is generated. Only one outstanding DNS update operation is allowed.

Examples

The following example performs a DNS update:

```
ciscoasa# dns update
ciscoasa# ...
ciscoasa# [Done] dns update
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.

Command	Description
dns server-group	Enters dns-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server group configurations.

domain

To configure a DNS domain name for a network-service object or object group, use the **domain** command in object configuration mode. Use the **no** form of this command to remove the domain from the configuration.

domain *domain_name* [*service*]
no domain *domain_name* [*service*]

Syntax Description

domain_name	The DNS name, up to 253 characters. This can be fully-qualified (such as www.example.com) or partial (such as example.com), in which case the object matches all subdomains, that is, servers with the partial name (such as www.example.com, www1.example.com, long.server.name.example.com, and so forth). Connections will be matched against the longest name if an exact match is available. The domain name can resolve to multiple IP addresses.
service	(Optional.) Specify the service only if you want to limit the scope of the connections matched. By default, any connection to the resolved IP addresses for the domain name matches the object. *protocol* [*operator port*] where: • *protocol* is the protocol used in the connection, such as tcp, udp, ip, and so forth. Use ? to see the list of protocols. • (TCP/UDP only.) *operator* is one of the following: • **eq** equals the port number specified. • **lt** means any port less than the specified port number. • **gt** means any port greater than the specified port number. • **range** means any port between the two ports specified. • (TCP/UDP only.) *port* is the port number, 1-65535 or a mnemonic, such as www. Use ? to see the mnemonics. For ranges, you must specify two ports, with the first port being a lower number than the second port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network-service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Usage Guidelines

You must configure DNS servers and enable domain lookup services on the device interfaces so that the system can request IP addresses for the domain names.

Example

The following example creates several network-service objects that include domain names.

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

Related Commands

Command	Description
object network-service	Creates a network-service object.
object-group network-service	Creates a network-service object group.

domain-name (dns server-group)

To set the default domain name to append to unqualified hostnames, use the **domain-name** command in dns server-group configuration mode. To remove the domain name, use the **no** form of this command.

domain-name*name*
no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Command Default

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dns server-group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the ASA qualifies the name to “jupiter.example.com.”

Examples

The following example sets the domain to “example.com” for “dnsgroup1”:

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters dns-server-group configuration mode, in which you can configure a DNS server group.
domain-name	Sets the default domain name globally.
show running-config dns-server group	Shows one or all the current DNS server group configurations.

domain-name (global)

To set the default domain name, use the **domain-name** command in global configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *name*
no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Command Default

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com" and specify a syslog server by the unqualified name of "jupiter," then the ASA qualifies the name to "jupiter.example.com." For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Examples

The following example sets the domain to example.com:

```
ciscoasa(config)# domain-name example.com
```

Related Commands

Command	Description
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Identifies a DNS server for the ASA.
hostname	Sets the ASA hostname.
show running-config domain-name	Shows the domain name configuration.

domain-name (ipv6 dhcp pool)

To provide the domain name to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **domain-name** command in ipv6 dhcp pool configuration mode. To remove the domain name, use the **no** form of this command.

domain-name*domain_name*
no domain-name *domain_name*

Syntax Description

domain_name	Specifies the domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the domain name, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
```

```
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.

Command	Description
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

domain-password

To configure the IS-IS routing domain authentication password, use the **domain-password** command in router isis configuration mode. To disable a password, use the **no** form of this command.

domain-name *password* [**authenticate snp** { **validate** | **send-only** }]
no domain-name *password*

Syntax Description

password	Password you assign.
authenticate snp	(Optional) Causes the system to insert the password into SNP PDUs.
validate	(Optional) Causes the system to insert the password into the SNPs and check the password in SNPs that it receives.
send-only	(Optional) Causes the system only to insert the password into the SNPs, but not check the password in SNPs that it receives. Use this keyword during a software upgrade to ease the transition.

Command Default

No domain password is specified and no authentication is enabled for exchange of Level 2 routing information.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This password is exchanged as plain text and thus this feature provides only limited security.

This password is inserted in Level 2 (area router level) PDU link-state packets (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

If you do not specify the **authenticate snp** keyword along with either the **validate** or **send-only** keyword, then the IS-IS routing protocol does not insert the password into SNPs.

Examples

The following example assigns an authentication password to the routing domain and specifies that the password be inserted in SNPs and checked in SNPs that the system receives:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.

Command	Description
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.

Command	Description
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

downgrade

To downgrade your software version, use the **downgrade** command in global configuration mode.

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

Syntax Description

activation-key *old_key*	(Optional) If you need to revert the activation key, then you can enter the old activation key.
old_config_url	Specifies the path to the saved, pre-migration configuration (by default this was saved on disk0).
old_image_url	Specifies the path to the old image on disk0, disk1, tftp, ftp, or smb.
/noconfirm	(Optional) Downgrades without prompting.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

This command is a shortcut for completing the following functions:

1. Clearing the boot image configuration (**clear configure boot**).
2. Setting the boot image to be the old image (**boot system**).
3. (Optional) Entering a new activation key (**activation-key**).
4. Saving the running configuration to startup (**write memory**). This sets the BOOT environment variable to the old image, so when you reload, the old image is loaded.
5. Copying the old configuration to the startup configuration (**copy** *old_config_url* **startup-config**).
6. Reloading (**reload**).

Examples

The following example downgrades without confirming:

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

Related Commands

Command	Description
activation-key	Enters an activation key.
boot system	Sets the image to boot from.
clear configure boot	Clears the boot image configuration.
copy startup-config	Copies a configuration to the startup configuration.

download-max-size

Note The **download-max-size** command does not work. Do not use it. However, you might see it in the running configuration, and it is available in the CLI.

To specify the maximum size allowed for an object to download, use the **download-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

download-max-size*size*
no download-max-size

Syntax Description

size	Specifies the maximum size allowed for a downloaded object. The range is 0 through 2147483647. Setting the size to 0 effectively disallows object downloading.

Command Default

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example sets the maximum size for a downloaded object to 1500 bytes:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
download-max-size 1500
```

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
upload-max-size	Specifies the maximum size of an object to upload.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

drop

To drop all packets that match the **match** command or **class** command, use the **drop** command in match or class configuration mode. To disable this action, use the no form of this command.

drop [**send-protocol-error**] [**log**]
no drop [**send-protocol-error**] [**log**]

Syntax Description

log	Logs the match. The syslog message number depends on the application.
send-protocol-error	Sends a protocol error message.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When using the Modular Policy Framework, drop packets that match a **match** command or class map by using the **drop** command in match or class configuration mode. This drop action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop** command to drop all packets that match the **match** command or **class** command.

If you drop a packet, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets and sends a log when they match the HTTP traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

drop-connection

When using the Modular Policy Framework, drop packets and close the connection for traffic that matches a **match** command or class map by using the **drop-connection** command in match or class configuration mode. To disable this action, use the no form of this command.

drop-connection [**send-protocol-error**] [**log**]
no drop-connection [**send-protocol-error**] [**log**]

Syntax Description

send-protocol-error	Sends a protocol error message.
log	Logs the match. The system log message number depends on the application.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Match and class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The connection will be removed from the connection database on the ASA. Any subsequent packets entering the ASA for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop-connection** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you drop a packet or close a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet and close the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop-connection** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action. For example, enter the **inspect http http_policy_map** command, where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets, closes the connection, and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

dtls port

To specify a port for DTLS connections, use the **dtls port** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of this command:

dtls port *number*
no dtls port *number*

Syntax Description

number	The UDP port number, from 1 to 65535.

Command Default

The default port number is 443.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This command specifies the UDP port to be used for SSL VPN connections using DTLS.

DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Examples

The following example enters webvpn configuration mode and specifies port 444 for DTLS:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

Related Commands

Command	Description
dtls enable	Enables DTLS on an interface.
svc dtls	Enables DTLS for groups or users establishing SSL VPN connections.
vpn-tunnel-protocol	Specifies VPN protocols that the ASA allows for remote access, including SSL.

duplex

To set the duplex of a copper (RJ-45) Ethernet interface, use the **duplex** command in interface configuration mode. To restore the duplex setting to the default, use the **no** form of this command.

duplex { **auto** | **full** | **half** }
no duplex

Syntax Description

auto	Auto-detects the duplex mode.
full	Sets the duplex mode to full duplex.
half	Sets the duplex mode to half duplex.

Command Default

The default is auto detect.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the duplex mode on the physical interface only.

The **duplex** command is not available for fiber media.

If your network does not support auto detection, set the duplex mode to a specific value.

For RJ-45 interfaces on the ASA 5500 series, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the duplex to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the duplex mode to full duplex:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

dynamic-access-policy-config

To configure a DAP record and the access policy attributes associated with it, use the **dynamic-access-policy-config** command in global configuration mode. To remove an existing DAP configuration, use the **no** form of this command.

dynamic-access-policy-config *name* | *activate*
no dynamic-access-policy-config

Syntax Description

activate	Activates the DAP selection configuration file.
name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration (name)	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC (activate)	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **dynamic-access-policy-config** command in global configuration mode to create one or more DAP records. To activate a DAP selection configuration file, use the **dynamic-access-policy-config** command with the *activate* argument.

When you use this command, you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- **action**
- **description**
- **network-acl**

- **priority**
- **user-message**
- **webvpn**

Examples

The following example shows how to configure the DAP record named user1:

```
ciscoasa
(config)
# dynamic-access-policy-config user1
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Populates the DAP record with access policy attributes.
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

dynamic-access-policy-record

To create a DAP record and populate it with access policy attributes, use the **dynamic-access-policy-record** command in global configuration mode. To remove an existing DAP record, use the **no** form of this command.

dynamic-access-policy-record*name*
no dynamic-access-policy-record *name*

Syntax Description

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **dynamic-access-policy-record** command in global configuration mode to create one or more DAP records. When you use this command, you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- **action** (**continue**, **terminate**, or **quarantine**)
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

Examples

The following example shows how to create a DAP record named Finance.

```
ciscoasa
(config)
```

```
# dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
clear config dynamic-access-policy-record	Removes all DAP records or the named DAP record.
dynamic-access-policy-config url	Configures the DAP Selection Configuration file.
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

dynamic-authorization

To enable RADIUS dynamic authorization (change of authorization) services for the AAA server group, use the **dynamic-authorization** command in aaa-server group configuration mode. To disable dynamic authorization, use the **no** form of this command.

dynamic-authorization [**port** *number*]
no dynamic-authorization [**port** *number*]

Syntax Description

port *number*	(Optional) Specifies the dynamic authorization port on the ASA. It can range from 1024 to 65535.

Command Default

The default listening port is 1700. By default dynamic-authorization is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server group configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure a RADIUS server group for ISE Change of Authorization (CoA). Once defined, the corresponding RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from ISE.

The ISE Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is established. When a policy changes for a user or user group in AAA, CoA packets can be sent directly to the ASA from the ISE to reinitialize authentication and apply the new policy. An Inline Posture Enforcement Point (IPEP) is no longer required to apply access control lists (ACLs) for each VPN session established with the ASA.

When an end user requests a VPN connection, the ASA authenticates the user to the ISE and receives a user ACL that provides limited access to the network. An accounting start message is sent to the ISE to register the session. Posture assessment occurs directly between the NAC agent and the ISE. This process is transparent to the ASA. The ISE sends a policy update to the ASA via a CoA “policy push.” This identifies a new user ACL that provides increased network access privileges. Additional policy evaluations may occur during the lifetime of the connection, transparent to the ASA, via subsequent CoA updates.

Examples

The following example shows how to configure an ISE server group for dynamic authorization (CoA) updates and hourly periodic accounting. Included is the tunnel group configuration that configures password authentication with ISE.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. In this case, you include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

Related Commands

Command	Description
authorize-only	Enables authorize-only mode for the RADIUS server group.
interim-accounting-update	Enables the generation of RADIUS interim-accounting-update messages.
without-csd	Switches off hostscan processing for connections that are made to a specific tunnel-group.

dynamic-filter ambiguous-is-black

To treat Botnet Traffic Filter greylisted traffic as blacklisted traffic for dropping purposes, use the **dynamic-filter ambiguous-is-black** command in global configuration mode. To allow greylisted traffic, use the **no** form of this command.

dynamic-filter ambiguous-is-black
no dynamic-filter ambiguous-is-black

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

If you configured the **dynamic-filter enable** command and then the **dynamic-filter drop blacklist** command, this command treats greylisted traffic as blacklisted traffic for dropping purposes. If you do not enable this command, greylisted traffic will not be dropped.

Ambiguous addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the greylist.

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops blacklisted and greylisted traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.

Command	Description
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.

Command	Description
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter blacklist

To edit the Botnet Traffic Filter blacklist, use the **dynamic-filter blacklist** command in global configuration mode. To remove the blacklist, use the **no** form of this command.

dynamic-filter blacklist
no dynamic-filter blacklist

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

After you enter the dynamic-filter blacklist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist using the **address** and **name** commands. You can also enter names or IP addresses in a whitelist (see the **dynamic-filter whitelist** command), so that names or addresses that appear on both the dynamic blacklist and whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist.

Static blacklist entries are always designated with a Very High threat level.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the *DNS host cache* . (This action is a background process, and does not affect your ability to continue configuring the ASA). We recommend also enabling DNS packet inspection with Botnet Traffic Filter snooping (see the **inspect dns dynamic-filter-snooping** command). The ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the 1-minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

The static database lets you augment the dynamic database with domain names or IP addresses that you want to blacklist.

If you do not enable Botnet Traffic Filter snooping, and one of the above circumstances occurs, then that traffic will not be monitored by the Botnet Traffic Filter.



Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.

Command	Description
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database fetch

To test the download of the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter database fetch** command in privileged EXEC mode.

dynamic-filter database fetch

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The actual database is not stored on the ASA; it is downloaded and then discarded. Use this command for testing purposes only.

Examples

The following example tests the download of the dynamic database:

```
ciscoasa# dynamic-filter database fetch
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.

Command	Description
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database find

To check if a domain name or IP address is included in the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter database find** command in privileged EXEC mode.

dynamic-filter database find *string*

Syntax Description

string	The *string* can be the complete domain name or IP address, or you can enter part of the name or address, with a minimum search string of 3 characters. Regular expressions are not supported for the database search.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

If there are multiple matches, the first two matches are shown. To refine your search for a more specific match, enter a longer string.

Examples

The following example searches on the string “example.com,” and finds one match:

```
ciscoasa# dynamic-filter database find bad.example.com
   bad.example.com
Found 1 matches
```

The following example searches on the string “bad,” and finds more than two matches:

```
ciscoasa# dynamic-filter database find bad
   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

Related Commands

Command	Description
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.

Command	Description
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter database purge

To manually delete the Botnet Traffic Filter dynamic database from running memory, use the **dynamic-filter database purge** command in privileged EXEC mode.

dynamic-filter database purge

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The database files are stored in running memory; they are not stored in flash memory. If you need to delete the database, use the **dynamic-filter database purge** command.

Before you can purge the database files, disable use of the database using the **no dynamic-filter use-database** command.

Examples

The following example disables use of the database, and then purges the database:

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.

Command	Description
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter drop blacklist

To automatically drop blacklisted traffic using the Botnet Traffic Filter, use the **dynamic-filter drop blacklist** command in global configuration mode. To disable the automatic dropping, use the **no** form of this command.

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** { **eq** *level* | **range** *min max* }]
no dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** { **eq** *level* | **range** *min max* }]

Syntax Description

action-classify-list *sub_access_list*	(Optional) Identifies a subset of traffic that you want to drop . See the **access-list extended** command to create the access list. The dropped traffic must always be equal to or a subset of the monitored traffic identified by the **dynamic-filter enable** command. For example, if you specify an access list for the **dynamic-filter enable** command, and you specify the **action-classify-list** for this command, then it must be a subset of the **dynamic-filter enable** access list.
interface *name*	(Optional) Limits monitoring to a specific interface. The dropped traffic must always be equal to or a subset of the monitored traffic identified by the **dynamic-filter enable** command. Any interface-specific commands take precedence over the global command.
threat-level {**eq** *level* | **range** *min max* }	(Optional) Limits the traffic dropped by setting the threat level. If you do not explicitly set a threat level, the level used is **threat-level range moderate very-high**. **Note** We highly recommend using the default setting unless you have strong reasons for changing the setting. The *level* and *min* and *max* options are: • **very-low** • **low** • **moderate** • **high** • **very-high** **Note** Static blacklist entries are always designated with a Very High threat level.

Command Default

This command is disabled by default.

The default threat level is **threat-level range moderate very-high**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

Be sure to first configure a **dynamic-filter enable** command for any traffic you want to drop; the dropped traffic must always be equal to or a subset of the monitored traffic.

You can enter this command multiple times for each interface and global policy. Make sure you do not specify overlapping traffic in multiple commands for a given interface/global policy. Because you cannot control the exact order that commands are matched, overlapping traffic means you do not know which command will be matched. For example, do not specify both a command that matches all traffic (without the **action-classify-list** keyword) as well as a command with the **action-classify-list** keyword for a given interface. In this case, the traffic might never match the command with the **action-classify-list** keyword. Similarly, if you specify multiple commands with the **action-classify-list** keyword, make sure each access list is unique, and that the networks do not overlap.

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.

Command	Description
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter enable

To enable the Botnet Traffic Filter, use the **dynamic-filter enable** command in global configuration mode. To disable the Botnet Traffic Filter, use the **no** form of this command.

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]
no dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

Syntax Description

classify-list *access_list*	Identifies the traffic that you want to monitor using an extended access list (see the **access-list extended** command). If you do not create an access list, by default you monitor all traffic.
interface *name*	Limits monitoring to a specific interface.

Command Default

The Botnet Traffic Filter is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The Botnet Traffic Filter compares the source and destination IP address in each initial connection packet to the IP addresses in the dynamic database, static database, DNS reverse lookup cache, and DNS host cache, and sends a syslog message or drops any matching traffic.

Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.”

The DNS snooping is enabled separately (see the **inspect dns dynamic-filter-snoop** command). Typically, for maximum use of the Botnet Traffic Filter, you need to enable DNS snooping, but you can use Botnet Traffic Filter logging independently if desired. Without DNS snooping for the dynamic database, the Botnet Traffic Filter uses only the static database entries, plus any IP addresses in the dynamic database; domain names in the dynamic database are not used.

Botnet Traffic Filter Address Categories

Addresses monitored by the Botnet Traffic Filter include:

- Known malware addresses—These addresses are on the "blacklist."
- Known allowed addresses—These addresses are on the "whitelist."
- Ambiguous addresses—These addresses are associated with multiple domain names, but not all of these domain names are on the blacklist. These addresses are on the "greylist."
- Unlisted addresses—These addresses are unknown, and not included on any list.

Botnet Traffic Filter Actions for Known Addresses

You can configure the Botnet Traffic Filter to log suspicious activity using the **dynamic-filter enable** conmmand, and you can optionally configure it to block suspicious traffic automatically using the **dynamic-filter drop blacklist** command.

Unlisted addresses do not generate any syslog messages, but addresses on the blacklist, whitelist, and greylist generate syslog messages differentiated by type. The Botnet Traffic Filter generates detailed syslog messages numbered 338*nnn* . Messages differentiate between incoming and outgoing connections, blacklist, whitelist, or greylist addresses, and many other variables. (The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.)

See the syslog messages guide for detailed information about syslog messages.

Device Support

You can enable the Botnet Traffic Filter on the following device models:

- ASA 5505
- ASA 5510, 5520, 5540, 5550
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X
- ASA 5580
- ASA 5585-X
- ASASM

Examples

The following example monitors all port 80 traffic on the outside interface, and then drops traffic at a threat level of moderate or greater:

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.

Command	Description
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter updater-client enable

To enable downloading of the dynamic database from the Cisco update server for the Botnet Traffic Filter, use the **dynamic-filter updater-client enable** command in global configuration mode. To disable downloading of the dynamic database, use the **no** form of this command.

dynamic-filter updater-client enable
no dynamic-filter updater-client enable

Syntax Description

This command has no arguments or keywords.

Command Default

Downloading is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

If you do not have a database already installed on the ASA, it downloads the database after approximately 2 minutes. The update server determines how often the ASA polls the server for future updates, typically every hour.

The Botnet Traffic Filter can receive periodic updates for the dynamic database from the Cisco update server.

This database lists thousands of known bad domain names and IP addresses. When the domain name in a DNS reply matches a name in the dynamic database, the Botnet Traffic Filter adds the name and IP address to the *DNS reverse lookup cache* . When the infected host starts a connection to the IP address of the malware site, then the ASA sends a syslog message informing you of the suspicious activity.

To use the database, be sure to configure a domain name server for the ASA so that it can access the URL. To use the domain names in the dynamic database, you need to enable DNS packet inspection with Botnet Traffic Filter snooping; the ASA looks inside the DNS packets for the domain name and associated IP address.

In some cases, the IP address itself is supplied in the dynamic database, and the Botnet Traffic Filter logs any traffic to that IP address without having to inspect DNS requests.

The database files are stored in running memory; they are not stored in flash memory. If you need to delete the database, use the **dynamic-filter database purge** command.

Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following multiple mode example enables downloading of the dynamic database, and enables use of the database in context1 and context2:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

The following single mode example enables downloading of the dynamic database, and enables use of the database:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns name-server	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.

Command	Description
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter use-database

To enable use of the dynamic database for the Botnet Traffic Filter, use the **dynamic-filter use-database** command in global configuration mode. To disable use of the dynamic database, use the **no** form of this command.

dynamic-filter use-database
no dynamic-filter use-database

Syntax Description

This command has no arguments or keywords.

Command Default

Use of the database is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

Disabling use of the downloaded database is useful in multiple context mode, so you can configure use of the database on a per-context basis. To enable downloading of the dynamic database, see the **dynamic-filter updater-client enable** command.

Examples

The following multiple mode example enables downloading of the dynamic database, and enables use of the database in context1 and context2:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

The following single mode example enables downloading of the dynamic database, and enables use of the database:

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

dynamic-filter whitelist

To edit the Botnet Traffic Filter whitelist, use the **dynamic-filter whitelist** command in global configuration mode. To remove the whitelist, use the **no** form of this command.

dynamic-filter whitelist
no dynamic-filter whitelist

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The static database lets you augment the dynamic database with domain names or IP addresses that you want to whitelist. After you enter the dynamic-filter whitelist configuration mode, you can manually enter domain names or IP addresses (host or subnet) that you want to tag as good names in a whitelist using the **address** and **name** commands. Names or addresses that appear on both the dynamic blacklist and static whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist. You can enter names or IP addresses in the static blacklist using the **dynamic-filter blacklist** command.

When you add a domain name to the static database, the ASA waits 1 minute, and then sends a DNS request for that domain name and adds the domain name/IP address pairing to the *DNS host cache* . (This action is a background process, and does not affect your ability to continue configuring the ASA). We recommend also enabling DNS packet inspection with Botnet Traffic Filter snooping (see the **inspect dns dynamic-filter-snooping** command). The ASA uses Botnet Traffic Filter snooping instead of the regular DNS lookup to resolve static blacklist domain names in the following circumstances:

- The ASA DNS server is unavailable.
- A connection is initiated during the 1 minute waiting period before the ASA sends the regular DNS request.

If DNS snooping is used, when an infected host sends a DNS request for a name on the static database, the ASA looks inside the DNS packets for the domain name and associated IP address and adds the name and IP address to the DNS reverse lookup cache.

If you do not enable Botnet Traffic Filter snooping, and one of the above circumstances occurs, then that traffic will not be monitored by the Botnet Traffic Filter.



Note This command requires ASA use of a DNS server; see the **dns domain-lookup** and **dns server-group** commands.

Examples

The following example creates entries for the blacklist and whitelist:

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.

Command	Description
dynamic-filter use-database	Enables use of the dynamic database.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.