

HA Proxy DNS Configuration Mode Commands

Important HA Proxy DNS Intercept is a license-enabled feature.

Command Modes The HA Proxy DNS Configuration Mode is used to create rules for Home Agent (HA) proxy DNS intercept lists that redirect packets with unknown foreign DNS addresses to a home network DNS server.

Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

configure > context *context_name* **> proxy-dns intercept-list** *list_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-proxy-dns-intercept-list)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- description, on page 1
- end, on page 2
- exit, on page 2
- pass-thru, on page 2
- redirect, on page 3

description

Allows you to enter descriptive text for this configuration.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
description text
no description
```

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines The description should provide useful information about this configuration.

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

pass-thru

Sets IP addresses that should be allowed through the proxy DNS intercept feature.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

configure > context *context_name* **> proxy-dns intercept-list** *list_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-proxy-dns-intercept-list)#
```

Syntax Description

[no] pass-thru { *ipv4_address* | *ipv6_address* } [/*ip_mask*]

no

Removes the DNS IP address from the pass-thru rule.

pass-thru *ip_address* [/*ip_mask*]

Specifies an DNS IP address that is allowed through the intercept feature.

ip_address [/*ip_mask*]: Specifies the IP address and network mask bits. *ip_address* [/*ip_mask*] is specified using IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation. The mask bits are a numeric value which is the number of bits in the subnet mask (CIDR notation).

Usage Guidelines

Use this command to identify DNS IP addresses that should be allowed through the intercept feature. For a more detailed explanation of the proxy DNS intercept feature, see the **proxy-dns intercept-list** command in the *Context Configuration Mode Commands* chapter. A maximum of 16 intercept rules (either **redirect** or **pass-thru**) are allow for each intercept list.



Important To allow packets through that do not match either the **pass-thru** or **redirect** rules, set a **pass-thru** rule address as: 0.0.0.0/0. If a packet does not match either the **pass-thru** or **redirect** rule, the packet is dropped.

Example

The following command allows a foreign network's DNS with an IP address of *10.2.55.12* to avoid being redirected:

```
pass-thru 10.2.55.12
```

redirect

Redirects DNS IP addresses from foreign networks matching an IP address in this command to a home network DNS.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

configure > context *context_name* **> proxy-dns intercept-list** *list_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-proxy-dns-intercept-list)#
```

Syntax Description

```
redirect { ipv4_address | ipv6_address } [ primary-dns { ipv4_address | ipv6_address
 } + | [ secondary-dns { ipv4_address | ipv6_address } + ] ]
no redirect { ipv4_address | ipv6_address }
```

no

Removes the DNS IP address from the redirect rule.

primary-dns { *ipv4_address* | *ipv6_address* } +

Specifies the IP address of the primary home network DNS.

ipv4_address must be an IPv4 address in dotted-decimal notation.

ipv6_address must be an IPv6 address in colon-separated hexadecimal notation.

+ indicates that the keyword and variable option can be used multiple times in the same command.

secondary-dns { *ipv4_address* | *ipv6_address* } +

Specifies the IP address of the secondary home network DNS.

ipv4_address must be an IPv4 address in dotted-decimal notation.

ipv6_address must be an IPv6 address in colon-separated hexadecimal notation.

+ indicates that the keyword and variable option can be used multiple times in the same command.

Usage Guidelines

Use this command to identify DNS IP addresses from foreign networks that are to be redirected to the home DNS. For a more detailed explanation of the Proxy DNS feature, see the proxy-dns intercept-list command in the *Context Configuration Mode Commands* chapter. A maximum of 16 intercept rules (either **redirect** or **pass-thru**) are allow for each intercept list.

Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command **ip dns-proxy source-address**.



Important If a packet does not match the **pass-thru** or **redirect** rule, the packet is dropped. If **primary-dns** or **secondary-dns** is not configured, DNS messages are redirected to the primary-dns-server (or the secondary-dns-server) configured for the subscriber OR inside the context.

Example

The following command identifies a foreign network DNS with an IP address of *209.165.200.236* and redirects it to a primary home network DNS with an IP address of *209.165.201.5*:

```
redirect 209.165.200.236 primary-dns 209.165.201.5 primary-dns
209.165.202.133 secondary-dns 209.165.201.2
```