Chapter 11. High Availability

This chapter describes the high availability fault-tolerance feature in D-Link Firewalls.

- Overview, page 289
- High Availability Mechanisms, page 291
- High Availability Setup, page 293
- High Availability Issues, page 296

11.1. Overview

High Availability is a fault-tolerant capability that is available on certain models of D-Link Firewalls. Currently the firewalls that offer this feature are the DFL-1600 and DFL-2500 models. The pre-installed licenses for these models include HA support.

HA Clusters

D-Link High Availability (HA) works by adding a back-up slave D-Link Firewall to an existing master firewall. The master and slave are connected together and make up a logical HA Cluster. One of the units in a cluster will be active when the other unit is inactive and on standby. Initially the slave will be inactive and will monitor the master. If the slave detects that the master is not responding, a failover takes place and the slave becomes active. If the master later regains full functionality the slave will continue to be active, with the master now monitoring the slave and failover only taking place if the slave fails. This is sometimes known as an active-passive HA implementation.

The Master and Active Units

It should be kept in mind that the master unit in a cluster is not always the same as the active unit. The active unit is the D-Link Firewall that is processing all traffic at a given point in time. This could be the slave if a failover has occurred because the master’s operation has been impaired.

Inter-connection

In a cluster, the master and slave units must be directly connected to each other by a synchronization connection which is known to NetDefendOS as the sync interface. One of the normal interfaces on the master and the slave are dedicated for this purpose and are connected together with a crossover cable.

Cluster Management

An HA Cluster of two D-Link Firewalls is managed as a single unit with a unique cluster name which appears in the management interface as a single logical D-Link Firewall. Administration operations such as changing rules in the IP rule set are carried out as normal with the changes automatically being made to the configurations of both the master and the slave.

Load-sharing

D-Link HA clusters do not provide load-sharing since only one unit will be active while the other is inactive and only two D-Link Firewalls, the master and the slave, can exist in a single cluster. The only processing function the inactive unit fulfills is to replicate the state of the active unit and to take over all traffic processing if it detects the active unit is not responding.

Hardware Duplication
11.1. Overview

D-Link HA will only operate between two D-Link Firewalls. As the internal operation of different security gateway manufacturer's software is completely dissimilar, there is no common method available to communicating state information to a dissimilar device.

It is also strongly recommended that the D-Link Firewalls used in cluster have identical configurations. They must also have identical licenses which allow identical capabilities including the ability to run in an HA cluster.

**Extending Redundancy**

Implementing an HA Cluster will eliminate one of the points of failure in a network. Routers, switches and Internet connections can remain as potential points of failure and redundancy for these should also be considered.

The following sections describe the High Availability feature in greater detail.
11.2. High Availability Mechanisms

D-Link HA provides a redundant, state-synchronized hardware configuration. The state of the active unit, such as the connection table and other vital information, is continuously copied to the inactive unit via the **sync** interface. When cluster failover occurs, the inactive unit knows which connections are active, and traffic can continue to flow.

The inactive system detects that the active system is no longer operational when it no longer detects sufficient **Cluster Heartbeats**. Heartbeats are sent over the **sync** interface as well as all other interfaces. NetDefendOS sends 5 heartbeats per second from the active system and when three heartbeats are missed (that is to say, after 0.6 seconds) a failover will be initiated. By sending heartbeats over all interfaces, the inactive unit gets an overall view of the active unit’s health. Even if **sync** is deliberately disconnected, failover may not result if the inactive unit receives enough heartbeats from other interfaces via a shared switch, however the **sync** interface sends twice as many heartbeats as any of the normal interfaces. The administrator can disable heartbeat sending on any of the interfaces.

Heartbeats are not sent at smaller intervals because such delays may occur during normal operation. An operation such as opening a file, could result in delays long enough to cause the inactive system to go active, even though the other is still active.

Cluster heartbeats have the following characteristics:

- The source IP is the interface address of the sending firewall
- The destination IP is the shared IP address
- The IP TTL is always 255. If NetDefendOS receives a cluster heartbeat with any other TTL, it is assumed that the packet has traversed a router, and hence cannot be trusted.
- It is a UDP packet, sent from port 999, to port 999.
- The destination MAC address is the ethernet multicast address corresponding to the shared hardware address. In other words, 11-00-00-C1-4A-nn. Link-level multicasts are used over normal unicast packets for security: using unicast packets would mean that a local attacker could fool switches to route heartbeats somewhere else so the inactive system never receives them.

The time for failover is typically about one second which means that clients may experience a failover as a slight burst of packet loss. In the case of TCP, the failover time is well within the range of normal retransmit timeouts so TCP will retransmit the lost packets within a very short space of time, and continue communication. UDP does not allow retransmission since it is inherently an unreliable protocol.

Both master and slave know about the shared IP address. ARP queries for the shared IP address, or any other IP address published via the ARP configuration section or through Proxy ARP, are answered by the active system. The hardware address of the shared IP address and other published addresses are not related to the actual hardware addresses of the interfaces. Instead the MAC address is constructed by NetDefendOS from the Cluster ID in the following form: 10-00-00-C1-4A-nn, where nn comes from combining the Cluster ID configured in the Advanced Settings section with the hardware bus/slot/port of the interface. The Cluster ID must be unique for each cluster in a network.

As the shared IP address always has the same hardware address, there will be no latency time in updating ARP caches of units attached to the same LAN as the cluster when failover occurs.

When a cluster member discovers that its peer is not operational, it broadcasts gratuitous ARP queries on all interfaces using the shared hardware address as the sender address. This allows switches to re-learn within milliseconds where to send packets destined for the shared address. The only delay in failover therefore, is detecting that the active unit is down.

ARP queries are also broadcast periodically to ensure that switches don't forget where to send
packets destined for the shared hardware address.
11.3. High Availability Setup

This section provides a step-by-step guide for setting up an HA Cluster.

11.3.1. Hardware Setup

1. Start with two physically similar D-Link Firewalls. Both may be newly purchased or one may have been purchased to be the back-up unit (in other words, to be the slave unit).

2. Make the physical connections:
   - Connect the matching interfaces of master and slave through a common switch.
   - Select an interface on the master and slave which is to be used by the units for monitoring each other and connect them together with an Ethernet crossover cable. This will be the NetDefendOS sync interface. It is recommended that the same interface is used on both master and slave, assuming they are similar systems.

Figure 11.1. High Availability Setup

The illustration above shows the typical HA Cluster connections. All interfaces of the master would normally also be present on the slave and be connected to the same networks. This is achieved by connecting the same interfaces on both master and slave via a switch to other network portions. The lan interface on the master and the lan interface on the slave would be connected to the same switch which then connects to an internal network. Similarly the wan interface on the master and the wan interface would connect to a switch which then connects to the external Internet.
3. Decide on a shared IP address for each interface in the cluster. Some interfaces could have shared addresses only with others having unique individual addresses as well. The shared and unique addresses are used as follows:

- The unique, non-shared IP addresses are used to communicate with the D-Link Firewalls themselves for functions such as remote control and monitoring. They can also be "pinged". They should not be associated with the traffic flowing through the cluster. If either unit is inoperative, the associated IP address will be unreachable. ARP queries for the respective addresses are answered by the firewall that owns the IP address, using the normal hardware address, just like normal IP units.

- One shared IP address is used for routing and it is also the address used by dynamic address translation, unless the configuration explicitly specifies another address.

Note
The shared IP address should not be used for remote management or monitoring purposes. When using, for example, SSH for remote management of the D-Link Firewalls in an HA Cluster, the individual IP addresses of the firewalls should be used.

11.3.2. NetDefendOS Setup

The remaining steps to configure the NetDefendOS software through the WebUI are as follows.

1. Connect to the master unit with the WebUI.
2. Go to System > High Availability
3. Check the Enable High Availability checkbox
4. Set the Cluster ID. This must be unique for each cluster.
5. Choose the Sync Interface
6. Select the node type to be Master
7. Go to Objects > Address book and create an IP4 HA address object for each interface. Each object must contain the master and slave IP address.
8. Go to Interfaces > Ethernet, going through each interface in the list and entering the shared IP address for that interface in the IP Address field.

Also select the Advanced tab for each interface and set the High Availability Private IP Address field to be the name of the IP4 HA object defined in the previous step for the interface (NetDefendOS will automatically select the appropriate address from the master and slave IP addresses defined for the object).

9. Repeat the above steps for the other D-Link Firewall but select the node type to be Slave.

The configuration on both D-Link Firewalls needs to be the same. Configurations between the units are automatically synchronized. To change something in a configuration logon to either the master or the slave, make the change then deploy. The changes are automatically made to both units.

11.3.3. Verifying Cluster Functioning

To verify that the cluster is performing correctly, first use an ha command on each unit. The output will look similar to this for the master:

```
> ha
```
This device is an HA MASTER
This device is currently ACTIVE (will forward traffic)
HA cluster peer is ALIVE

Then use the stat command to verify that both master and slave have about the same number of connections. The output should contain a line similar to this:

Connections 2726 out of 128000

where the lower number is the current number of connections and the higher number is the connections limit of the license.

The following points are also relevant to cluster setup:

• If this is not the first cluster in a network then the advanced setting ClusterID must be changed to have a unique value (the default is 0). This makes sure the MAC address for the cluster is unique.

• Enabling the advanced setting HAUseUniqueSharedMacAddressPerInterface is also recommended so that each interface has its own MAC address. If this is not enabled, interfaces share a MAC address and this can confuse some switches.

• Make sure that the advanced setting HighBuffers is set to automatic on all units in a cluster. This setting allocates memory for handling connections.

Where a cluster has tens of thousands of simultaneous connections then it may be necessary to set a value above the automatic value. Much higher values have the disadvantage of possibly increasing throughput latency.
11.4. High Availability Issues

The following points should be kept in mind when managing and configuring an HA Cluster.

**SNMP**

SNMP statistics are not shared between master and slave. SNMP managers have no failover capabilities. Therefore both firewalls in a cluster need to be polled separately.

**Using Individual IPs**

The unique individual IP addresses of the master and slave cannot safely be used for anything but management. Using them for anything else such as for source IPs in dynamically NATed connections or publishing services on them, will inevitably cause problems, as unique IPs will disappear when the firewall it belongs to does.

**Failed Interfaces**

Failed interfaces will not be detected unless they fail to the point where NetDefendOS cannot continue to function. This means that failover will not occur if the active unit can still send “am alive” heartbeats to the inactive unit through any of its interfaces, even though one or more interfaces may be inoperative.

**Changing the Cluster ID**

Changing the cluster ID in a live environment is not recommended for two reasons. Firstly this will change the hardware address of the shared IPs and will cause problems for all units attached to the local LAN, as they will keep the old hardware address in their ARP caches until it times out. Such units would have to have their ARP caches flushed.

Secondly this breaks the connection between the firewalls in the cluster for as long as they are using different configurations. This will cause both firewalls to go active at the same time.

**Invalid Checksums in Heartbeat Packets**

Cluster Heartbeats packets are deliberately created with invalid checksums. This is done so that they won’t be routed. Some routers may flag this invalid checksum in their log messages.
Chapter 12. ZoneDefense

This chapter describes the D-Link ZoneDefense feature.

• Overview, page 298
• ZoneDefense Switches, page 299
• ZoneDefense Operation, page 300

12.1. Overview

ZoneDefense allows a D-Link Firewall to control locally attached switches. It can be used as a counter-measure to stop a virus-infected computer in a local network from infecting other computers.

When hosts or clients on a network become infected with viruses or another form of malicious code, this can often show its presence through anomalous behaviour, often by large numbers of new connections being opened to outside hosts.

By setting up Threshold Rules, hosts or networks that are exceeding a defined connection threshold can be dynamically blocked using the ZoneDefense feature. Thresholds are based on either the number of new connections made per second, or on the total number of connections being made. The connections may be made by either a single host or all hosts within a specified CIDR network range (an IP address range specified by a combination of an IP address and its associated network mask).

When NetDefendOS detects that a host or a network has reached the specified limit, it uploads Access Control List (ACL) rules to the relevant switches and this blocks all traffic for the host or network displaying the unusual behaviour. Blocked hosts and networks remain blocked until the system administrator manually unblocks them using the Web or Command Line interface.

Note

ZoneDefense is available on the D-Link DFL-800/860/1600/2500 models.
12.2. ZoneDefense Switches

Switch information regarding every switch that is to be controlled by the firewall has to be manually specified in the firewall configuration. The information needed in order to control a switch includes:

- The IP address of the management interface of the switch
- The switch model type
- The SNMP community string (write access)

The ZoneDefense feature currently supports the following switches:

- D-Link DES 3226S (minimum firmware: R4.02-B14)
- D-Link DES 3250TG (minimum firmware: R3.00-B09)
- D-Link DES 3326S (minimum firmware: R4.01-B39)
- D-Link DES 3350SR (minimum firmware: R1.02.035)
- D-Link DES 3526 (minimum firmware: R3.01-B23)
- D-Link DES 3550 (minimum firmware: R3.01-B23)
- D-Link DGS 3324SR (minimum firmware: R4.10-B15)

Note

Make sure that the switches have the minimum required firmware versions before activating ZoneDefense.
12.3. ZoneDefense Operation

12.3.1. SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol for complex network management. SNMP allows the managers and managed devices in a network to communicate with each other.

**SNMP Managers**

A typical managing device, such as a D-Link Firewall, uses the SNMP protocol to monitor and control network devices in the managed environment. The manager can query stored statistics from the controlled devices by using the *SNMP Community String*. This is similar to a userid or password which allows access to the device's state information. If the community string type is *write*, the manager will be allowed to modify the device's state.

**Managed devices**

The managed devices must be SNMP compliant, as are D-Link switches. They store state data in databases known as the Management Information Base (MIB) and provide the information to the manager upon receiving an SNMP query.

12.3.2. Threshold Rules

A threshold rule will trigger ZoneDefense to block out a specific host or a network if the connection limit specified in the rule is exceeded. The limit can be one of two types:

- **Connection Rate Limit** - This can be triggered if the rate of new connections per second to the firewall exceeds a specified threshold.

- **Total Connections Limit** - This can be triggered if the total number of connections to the firewall exceeds a specified threshold.

Threshold rules have parameters which are similar to those for IP Rules. These parameters specify what type of traffic a threshold rule applies to.

A single threshold rule has the parameters:

- Source interface and source network
- Destination interface and destination network
- Service
- Type of threshold: Host and/or network based

Traffic that matches the above criteria and causes the host/network threshold to be exceeded will trigger the ZoneDefense feature. This will prevent the host/networks from accessing the switch(es). All blocking in response to threshold violations will be based on the IP address of the host or network on the switch(es). When a network-based threshold has been exceeded, the source network will be blocked out instead of just the offending host.

For a general description of how Threshold Rules are specified and function, please see Section 10.2, “Threshold Rules”.

12.3.3. Manual Blocking and Exclude Lists
As a complement to threshold rules, it is also possible to manually define hosts and networks that are to be statically blocked or excluded. Manually blocked hosts and networks can be blocked by default or based on a schedule. It is also possible to specify which protocols and protocol port numbers are to be blocked.

Exclude Lists can be created and used to exclude hosts from being blocked when a threshold rule limit is reached. Good practice includes adding to the list the firewall's interface IP or MAC address connecting towards the ZoneDefense switch. This prevents the firewall from being accidentally blocked out.

**Example 12.1. A simple ZoneDefense scenario**

The following simple example illustrates the steps needed to set up ZoneDefense. It is assumed that all interfaces on the firewall have already been configured.

An HTTP threshold of 10 connections/second is applied. If the connection rate exceeds this limitation, the firewall will block the specific host (in network range 192.168.2.0/24 for example) from accessing the switch completely.

A D-Link switch model DES-3226S is used in this case, with a management interface address 192.168.1.250 connecting to the firewall's interface address 192.168.1.1. This firewall interface is added into the exclude list to prevent the firewall from being accidentally locked out from accessing the switch.

**Web Interface**

Add a new switch into ZoneDefense section:

1. Go to **Zone Defense > Switches > Add > ZoneDefense switch**
2. Now enter:
   - **Name**: switch1
   - **Switch model**: DES-3226S
   - **IP Address**: 192.168.1.250
3. For **SNMP Community** enter the **Write Community String** configured for the switch
4. Press **Check Switch** to verify the firewall can communicate with the switch and the community string is correct.
5. Click **OK**

Add the firewall's management interface into the exclude list:

1. Go to **Zone Defense > Exclude list**
2. For **Addresses** choose the object name of the firewall's interface address 192.168.1.1 from the **Available** list and put it into the **Selected** list.

3. Click **OK**

Configure an HTTP threshold of 10 connections/second:

1. Go to **Traffic Management > Threshold Rules > Add > Threshold Rule**
2. For the **Threshold Rule** enter:
   - **Name**: HTTP-Threshold
   - **Service**: http
3. For **Address Filter** enter:
   - **Source Interface**: The firewall's management interface
   - **Destination Interface**: any
   - **Source Network**: 192.168.2.0/24 (or the object name)
   - **Destination Network**: all-nets
4. Click **OK**

Specify the threshold, the threshold type and the action to take if exceeded:

1. Go to **Add > Threshold Action**
2. Configure the **Threshold Action** as follows:
   - **Action**: Protect
   - **Group By**: Host-based
   - **Threshold**: 10
   - Set the units for the threshold value to be **Connections/Second**
   - Tick the **Use ZoneDefense** checkbox
   - Click **OK**

### 12.3.4. Limitations

There are some differences in ZoneDefense operation depending on switch model. The first difference is the latency between the triggering of a blocking rule to the moment when switch(es) actually starts blocking out the traffic matched by the rule. All switch models require a short period of latency time to implement blocking once the rule is triggered. Some models can activate blocking in less than a second while some models may require a minute or more.

A second difference is the maximum number of rules supported by different switches. Some switches support a maximum of 50 rules while others support up to 800 (usually, in order to block a host or network, one rule per switch port is needed). When this limit has been reached no more hosts or networks will be blocked out.

**Important**

ZoneDefense uses a range of the ACL rule set on the switch. To avoid potential conflicts in these rules and guarantee the firewall's access control, it is strongly recommended that the administrator clear the entire ACL rule set on the switch before executing the ZoneDefense setup.
12.3.4. Limitations