

How to use the WAN2 to WAN2 to setup IPsec on DFL series

[Topology]:

Site_A WAN1(1.1.1.1)-----(1.1.1.2)DES-3828(3.3.3.2)-----(3.3.3.1)Site_B
WAN2(2.2.2.1)-----(2.2.2.2) (4.4.4.2)-----(4.4.4.1)

Site_A: Use DFL-860 firmware 2.26.02.05 and LAN1 of Site_A is 192.168.1.0/24

Site_B: Use DFL-860 firmware 2.26.02.05 and LAN1 of Site_B is 192.168.10.0/24

[Configuration]:

[Site A configuration]:

The screenshot shows the D-Link web interface for Site A configuration. The left sidebar shows the navigation tree with 'InterfaceAddresses' selected. The main content area displays a table of interface addresses:

Name	Address	User Auth Groups	Comments
dmz_ip	172.17.100.254		IPAddress of interface dmz
dmznet	172.17.100.0/24		The network on interface dmz
lan_ip	192.168.1.1		IPAddress of interface lan
lannet	192.168.1.0/24		The network on interface lan
wan1_dns1	0.0.0.0		Primary DNS server for interface wan1
wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1
wan1_gw	1.1.1.2		Default gateway for interface wan1
wan1_ip	1.1.1.1		IPAddress of interface wan1
wan1net	1.1.1.0/24		The network on interface wan1
wan2_ip	2.2.2.1		IPAddress of interface wan2
wan2net	2.2.2.0/24		The network on interface wan2

The screenshot shows the D-Link web interface for Site A configuration, specifically the 'key2' configuration page. The left sidebar shows the navigation tree with 'Authentication Objects' selected. The main content area displays the configuration for 'key2':

key2
PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

General

Name: key2

Shared Secret

Passphrase

Shared Secret: [Redacted] Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Confirm Secret: [Redacted]

Hexadecimal key

Passphrase: [Redacted]

Comments

Comments: [Redacted]

IPsec
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

General

Name: ipsec
 Local Network: lannet
 Remote Network: 192.168.10.0/24
 Remote Endpoint: 4.4.4.1
 Encapsulation mode: Tunnel
 IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: High
 IKE Lifetime: 28800 seconds
 IPsec Algorithms: High
 IPsec Lifetime: 3600 seconds
 IPsec Lifetime: 0 kilobytes

Comments

main
The system has a predefined main routing table. Alternate routing tables can be defined by the user.

Add Edit this object

#	Type	Interface	Network	Gateway	Local IP address	Metric	Monitor this route	Comments
1	Route	wan1	wan1net			100	No	Direct route for network wan1net over interface wan1.
2	Route	wan1	all-nets	wan1_gw		100	No	Default route over interface wan1.
3	Route	wan2	wan2net			100	No	Direct route for network wan2net over interface wan2.
4	Route	dmz	dmznet			100	No	Direct route for network dmznet over interface dmz.
5	Route	lan	lannet			100	No	Direct route for network lannet over interface lan.
6	Route	IPsec	192.168.10.0/24			90	No	Direct route for network 192.168.10.0/24 over interface IPsec.
7	Route	wan2	4.4.4.0/24	2.2.2.2		0	No	

Right-click on a row for additional options.

IP Rules
IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

Add

#	Name	Action	Src-If	Src-Net	Dest-If	Dest-Net	Service
1	LAN_IPsec	Allow	lan	all-nets	IPsec	all-nets	all_services
2	IPsec_LAN	Allow	IPsec	all-nets	lan	all-nets	all_services
3	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
4	IPsec_core	Allow	IPsec	all-nets	core	lan_ip	all_icmp
5	lan_to_wan1						

Right-click on a row for additional options.

[Site B configuration]:

D-Link
Building Networks for People

Home Configuration Tools Status Maintenance Logout

Logged in as administrator admin - 192.168.1.111

SiteB

- System
- Objects
 - Address book
 - InterfaceAddresses
 - ALG with AVWCF
 - Services
 - IP Pools
 - NAT Pools
 - Schedules
 - Authentication Objects
 - VPN Objects
 - HTTP Banner Files
- Rules
- Interfaces
- Routing
- DR / IPS
- User Authentication
- Traffic Management
- ZoneDefense

InterfaceAddresses
An address folder can be used to group related address objects for better overview.

Add Edit this object

Name	Address	User Auth Groups	Comments
dmz_ip	172.17.100.254		IPAddress of interface dmz
dmznet	172.17.100.0/24		The network on interface dmz
lan_ip	192.168.10.1		IPAddress of interface lan
lannet	192.168.10.0/24		The network on interface lan
wan1_dns1	0.0.0.0		Primary DNS server for interface wan1
wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1
wan1_gw	3.3.3.2		Default gateway for interface wan1.
wan1_ip	3.3.3.1		IPAddress of interface wan1
wan1net	3.3.3.0/24		The network on interface wan1
wan2_ip	4.4.4.1		IPAddress of interface wan2
wan2net	4.4.4.0/24		The network on interface wan2

Right-click on a row for additional options.

key
PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

General

General

Name:

Shared Secret

Passphrase

Shared Secret: Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Confirm Secret:

ⓘ A PSK containing non-ASCII characters might be encoded different on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.

Hexadecimal key

Passphrase:

⚠ Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments

Comments:

SiteB

IPsec
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

General

Name:

Local Network:

Remote Network:

Remote Endpoint:

Encapsulation mode:

IKE Config Mode Pool:

Algorithms

IKE Algorithms:

IKE Lifetime: seconds

IPsec Algorithms:

IPsec Lifetime: seconds

IPsec Lifetime: kilobytes

Comments

main
The system has a predefined main routing table. Alternate routing tables can be defined by the user.

Add Edit this object

#	Type	Interface	Network	Gateway	Local IP address	Metric	Monitor this route	Comments
1	Route	wan1	wan1net			100	No	Direct route for network wan1net over interface wan1.
2	Route	wan1	all-nets	wan1_gw		100	No	Default route over interface wan1.
3	Route	wan2	wan2net			100	No	Direct route for network wan2net over interface wan2.
4	Route	dmz	dmznet			100	No	Direct route for network dmznet over interface dmz.
5	Route	lan	lannet			100	No	Direct route for network lannet over interface lan.
6	Route	IPsec	192.168.1.0/24			90	No	Direct route for network 192.168.1.0/24 over interface IPsec.
7	Route	wan2	2.2.2.0/24	4.4.4.2		0	No	

ⓘ Right-click on a row for additional options.

IP Rules
IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

Add

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	LAN_IPsec	Allow	lan	all-nets	IPsec	all-nets	all_services
2	IPsec_LAN	Allow	IPsec	all-nets	lan	all-nets	all_services
3	ping_fw	Allow	lan	lan	lan	lan	ping-inbound
4	IPsec_core	Allow	IPsec	all-nets	core	lan_jp	all_icmp
5	lan_to_wan1						

Right-click on a row for additional options.

[Testing result]:

D-Link Firewall 2.26.02

Logged in as administrator
admin - 192.168.1.111

Home Configuration Tools Status Maintenance Logout

SiteB

System
Objects
Rules
Interfaces
Routing
IP / IPS
User Authentication
Traffic Management
ZoneDefense

Interface: Source Destination
IP Address:
Port:
Event:
Severity: (Any) Action: Category: (Any)
Free Text:
Search Reset

Internal Logging (1-13)

Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2010-10-26 10:42:02	Info	CONN 600002	IPsec_LAN	ICMP	IPsec lan	192.168.1.111 192.168.10.21		conn_close close
2010-10-26 10:42:00	Info	CONN 600001	IPsec_LAN	ICMP	IPsec lan	192.168.1.111 192.168.10.100		conn_open
2010-10-26 10:41:57	Warning	IP_PROTO 7000014	TTLonLowMulticast	UDP	lan	192.168.10.100 239.255.255.250	1261 1900	ttl_low drop
2010-10-26 10:41:54	Warning	IP_PROTO 7000014	TTLonLowMulticast	UDP	lan	192.168.10.100 239.255.255.250	1261 1900	ttl_low drop
2010-10-26 10:41:54	Info	CONN 600001	IPsec_LAN	ICMP	IPsec lan	192.168.1.111 192.168.10.21		conn_open
2010-10-26 10:41:52	Warning	RULE 6000051	Default_Rule	IGMP	lan	192.168.10.100 224.0.0.22		ruleset_drop_packet drop

Administrator: Command Prompt

```

ping 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time=2ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126

ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

>>ping 192.168.10.100

ping 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time=2ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126
Reply from 192.168.10.100: bytes=32 time=1ms TTL=126

ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
  
```

Local Area Connection Status

Network Connection Details

Network Connection Details:

Property	Value
Description	Intel(R) PRO/100 VE Network Connection
Physical Address	00-07-E9-39-2D-15
DHCP Enabled	No
IPv4 IP Address	192.168.1.111
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes



Log on SiteB.log