An integrated approach to VPN

Using GNAT Box VPN & mobile VPN Client solutions with mesh and hub/spoke network topologies

Rock solid security

A Virtual Private Network (VPN) allows a private and secure network connection over a potentially insecure public network. A VPN extends a company's ability to exchange data and communications confidentially anywhere that a public network is in place. Using a VPN, a company's employees, clients and partners can access necessary information without breaching the security of the internal network.

When properly implemented, VPNs provide secure end-to-end communication that is comparatively inexpensive, easy to implement and expandable.

Mobile VPN clients

Client to gateway VPNs allow small offices and mobile users to initiate a connection to a GTA Firewall gateway from firewall or host with a dynamically assigned IP address using an authorized login name and password. The GNAT Box Mobile VPN Client secures data communications sent from a desktop or laptop computer across a public or private TCP/IP network for client-to-gateway and client-to-client connections.

VPN limitations

Though simple for one connection, VPN design becomes complex as the network grows. Especially when using a central transit point or hub to connect remote offices, the number of networks connected by VPNs exponentially increases the amount of bandwidth and the number of security associations used.

For most companies, the quality of the Internet connection will govern how many VPNs can be set up and how well they function. VPN connection quality can be determined by looking at three factors: reliability, number of router hops and latency.

The larger your bandwidth requirement, the more important the quality of your Internet connection. To determine the amount of bandwidth required for your company's VPN connections, examine these factors: the number of users; types of applications; projected traffic and encryption overhead.

One consideration is, will all VPNs be utilized at the same time? In a configuration with multiple end points, but low utilization, the VPN bandwidth usage may never reach the potential maximum. This can reduce the amount of load on the VPN connections at a given time, increasing the number of VPNs that can be supported.

VPNs and network topology

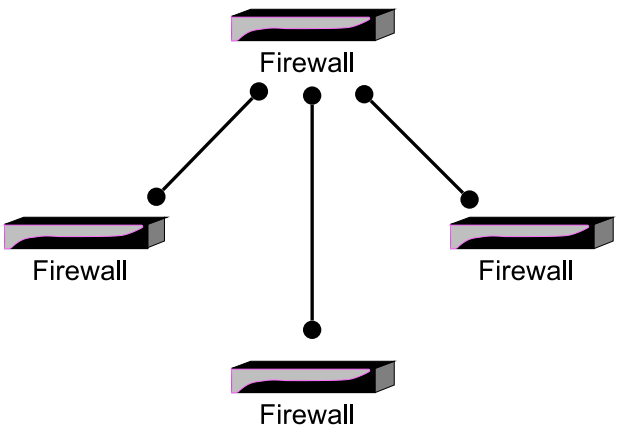
The network topology terms "mesh" and "hub and spoke," have come to be used in VPN connection design, but these terms can be misleading.

A mesh topology is a network architecture in which each end point is capable of reaching any other end point directly through a point-to-point circuit. The term "full mesh" refers to a network in which all end points are connected directly and no connection goes through a hub.

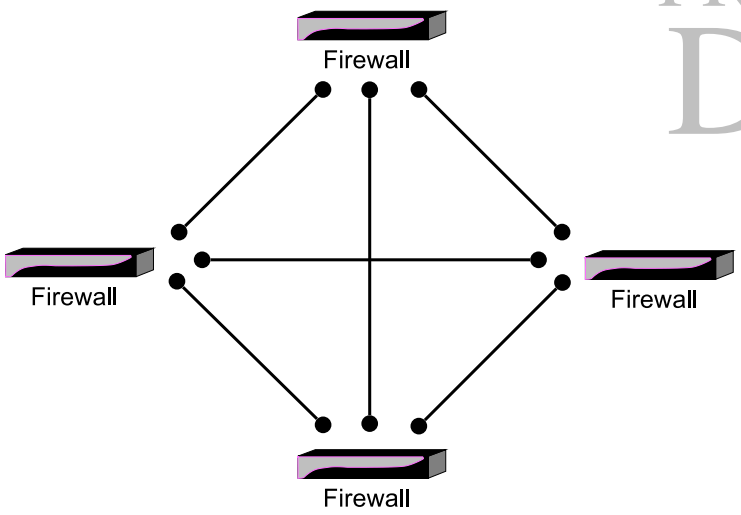
Hub and spoke topology, on the other hand, is a network architecture that uses a central connecting point. The hub is the connection point for any number of end points, and these end points or "spokes" may connect only to the hub, or may be connected through the hub to other end points.

VPNs in a network

VPNs don't necessarily follow the underlying network topology; they can be set up to connect directly or through a hub. Essentially, a VPN connection can be made directly from one site or



Hub & spoke network topology



Direct Connection VPN based on a mesh network topology

In a Direct Connection VPN, each VPN end point connects directly to each other end point, as represented by the connections in a mesh network topology, rather than through a transit point or hub.

client to another, (Direct Connection VPN), or it can be made from one site through a central transit point or hub to another site (Transit Point VPN). Below, we'll examine these two VPN topologies separately, but in practice, VPNs in a network should be set up in the most effective manner possible, using an efficient combination of connection topologies.

Direct Connection VPN

Direct Connection VPN is based on a mesh network topology connecting each site directly to the other sites. It can accommodate a network in which end points must communicate with one another without going through the main office firewall or the end points require connectivity only to the main office.

This VPN solution minimizes the number of paths for all VPN connections and the amount of potential VPN traffic with its encryption overhead. Direct Connection VPN reduces the number of security associations (SAs) used by the VPNs, reduces the potential time for a VPN to complete and simplifies VPN creation.

Characteristics

- Potentially easier VPN creation.
- Firewalls must have a number of VPNs adequate to the number of VPN connection end points.
- Firewalls must be powerful enough to support the maximum traffic these VPNs would generate.
- Multiple connection points.
- Failure of one end point does not affect other end points.

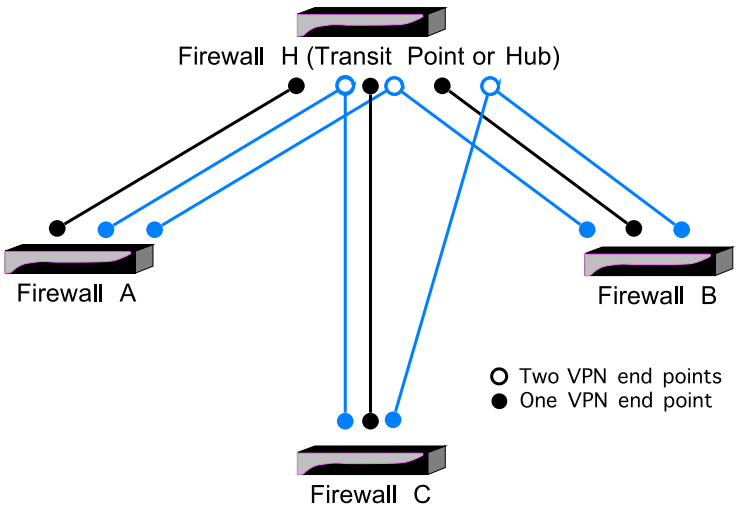
Transit Point (hub/spoke) VPN

A Transit Point VPN allows each remote site to connect directly to the hub, but only indirectly to the other sites. If most of the resources for a company are in a central network location with adequate bandwidth and connection speed to serve as a hub, a Transit Point VPN could be suitable.

In this VPN setup, the Transit Point or hub allows the remote offices to use the resources at the main office, but also routes traffic from one remote office or end point to another.

In the diagram shown, the Transit Point VPN is fully connected, meaning that each network can access each other network.

In the diagram, there is only one network per VPN end point. In practice, an end point may have multiple networks. Each network connected adds to the overhead for the VPN. Each segment of the communication path requires its own VPN, meaning that a connection for A–H requires one VPN and



Fully connected Transit Point (Hub) VPN

a connection for A–H–B requires two VPNs. The number of possible VPN security associations (SAs) can quickly be reached, either in potential bandwidth, or firewall VPN SA capacity.

A Transit Point VPN setup places the greatest load on the transit point/hub firewall. It utilizes more VPNs, therefore more SAs, and because the transit point firewall is the stopover for data that must be decrypted and then re-encrypted, a Transit Point VPN setup will have the potential to use more bandwidth than would a Direction Connection VPN in a configuration with the same number of end points.

GTA recommends using a GB-1500 as the transit point/hub firewall in a Transit Point VPN setup.

Packet in a Transit Point VPN

In a fully connected Transit Point VPN, (see diagram on page 4), a packet sent from Network A behind Firewall A to Network B behind Firewall B must pass through the transit point at the hub firewall. What happens to the packet as it passes through the transit point?

A packet sent from Network A destined for Network B is encrypted at Firewall A. From the External interface of Firewall A, the packet travels to the Hub Firewall's External interface where it is accepted or rejected; if rejected, it is dropped. If accepted, it is decrypted, and examined for its destination.

If the packet is destined for Network B behind Firewall B, it is re-encrypted and sent out the External interface to Firewall B. Here, the packet is accepted or rejected; if rejected, it is dropped. If the packet is accepted, it is decrypted, and sent to its destination on Network B behind Firewall B.

Characteristics

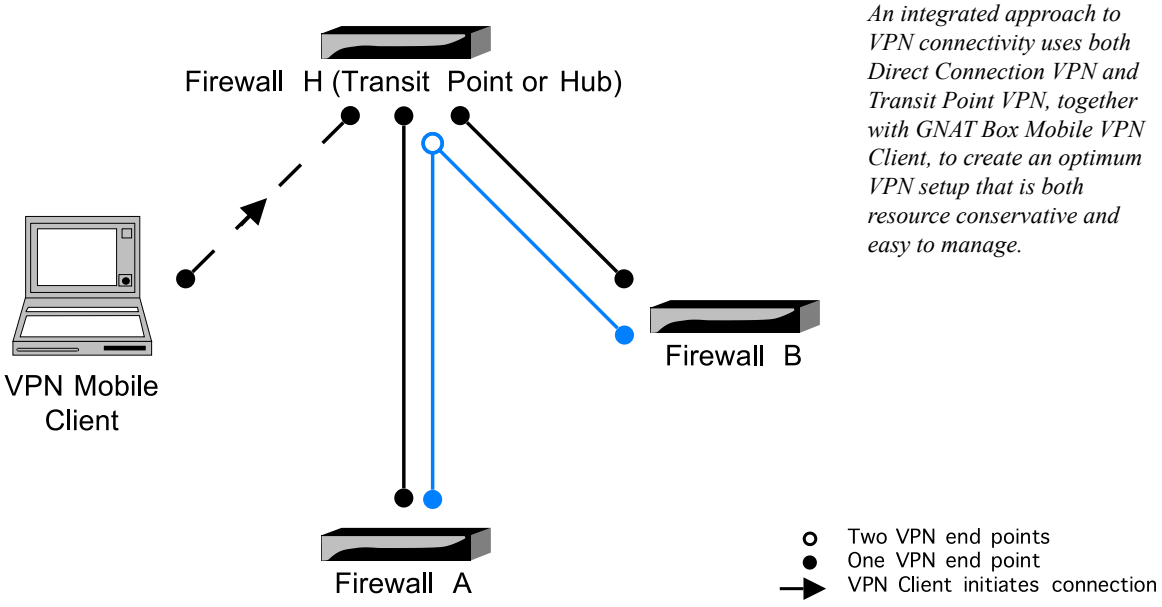
- Centralized VPN access control.
- Simpler remote office VPN configuration.
- Potentially more complex VPN object creation on all firewalls, and potentially more complex transit point VPN configuration.
- Transit point firewall must be able to provide enough VPNs for the number of end points.
- Transit point firewall must be powerful enough to support the maximum VPN traffic generated.
- Single point of failure.

Integrated VPN

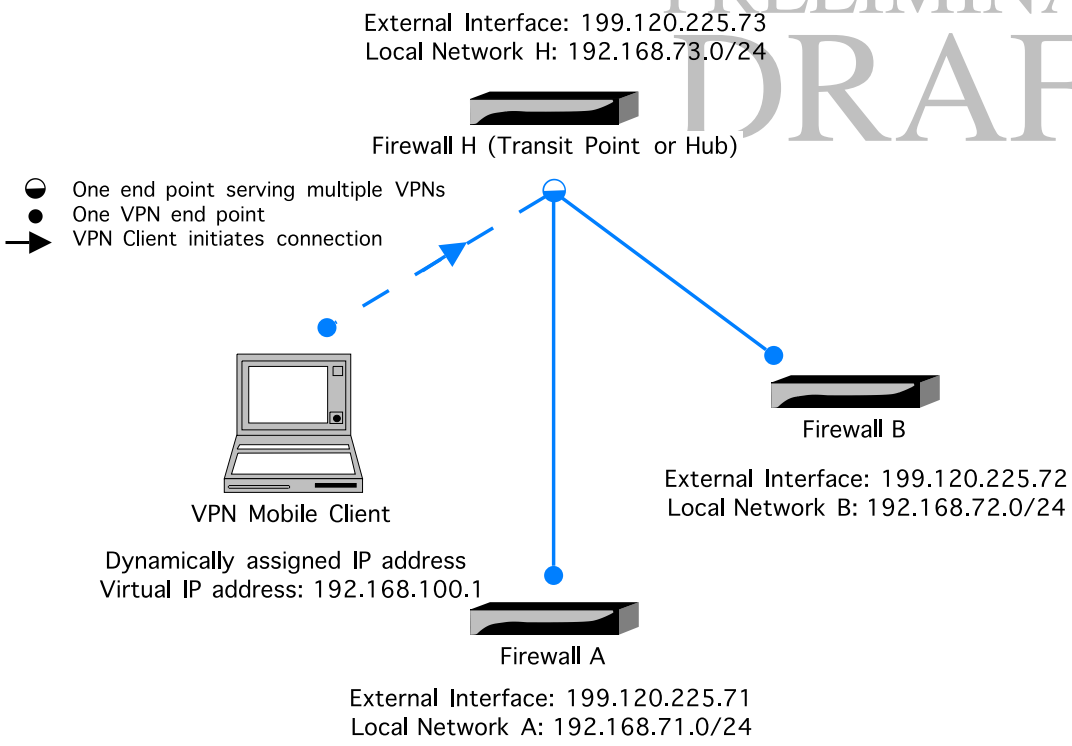
An integrated approach to creating VPNs, based on a partially meshed network topology, gives the administrator the ability to achieve functional VPNs in a real-world situation. It may be impossible to achieve ideal Internet connection quality, have a central site with adequate connection quality and resources, (as for a fully connected Transit Point VPN), or have remote sites capable of performing multiple VPN connections (as for a fully realized Direction Connection VPN).

Using an integrated approach, the requirements and limitations of each site are taken into account when choosing a direct or a transit point VPN connection. Integrated VPN creation combines the simplicity and flexibility of mesh network topology with the control of hub and spoke network topology.

For more information about VPNs, see VPN documentation on the web under Support/Documentation at http://www.gta.com/support2/documents/.



An integrated approach to VPN connectivity uses both Direct Connection VPN and Transit Point VPN, together with GNAT Box Mobile VPN Client, to create an optimum VPN setup that is both resource conservative and easy to manage.



Fully connected three-network VPN configuration using a hub

Supernet three networks & a mobile VPN client

in a fully connected Transit Point (hub/spoke) VPN

This example demonstrates how to use supernetting to configure VPNs for a network consisting of a transit point/hub firewall, firewalls A and B, and a mobile VPN client that will connect to both A and B through the transit point/hub.

Supernetting the entire corporate WAN/LAN structure allows for a simpler, more efficient VPN configuration. It also allows firewalls and remote networks to be added without changing the remote firewall configurations.

IP Pass Through filters shown in the example allow all access. Consult your corporate security policy for access restrictions through the established VPN.

Administration – v3.4.x and below

To administer a remote firewall locally in a supernetted configuration, the firewall can only be accessed using the IP address of the External interface.

Remote firewalls cannot be administered from their local network via the Protected interface. The VPN definition encompasses the firewall's local network range, so packets arriving at the Protected interface are compared to the VPN definition, and if matched, encrypted and sent through the VPN, where they cannot return to the Protected interface.

Other services running on the Protected interface such as DNS Proxy, DNS server, DHCP server, and the NTP server (if used by the local LAN), can also be affected by supernetting. (This issue does not affect the transit point/hub as the VPN definitions are specific to each remote network.)

As usual, secure remote firewall administration is possible via the External interface or through the VPN from the any firewall to each remote network with the appropriate Remote Access filter for remote administration.

Mobile VPN client

Mobile clients, as well as firewalls using the dynamic to static configuration, must initiate all VPN connections. For more information, see GTA's technical document **Connect from a Static to a Dynamic Gateway.**

The VPN client will follow the standard configuration outlined in the VPN documentation **GNAT Box VPN and VPN Client Feature Guide**. See an example illustration on page 8.

IP Addresses

Firewall A	199.120.225.71
Network A	192.168.71.0/24
Firewall B	199.120.225.72
Network B	192.168.72.0/24
Firewall Hub	199.120.225.73
Network Hub	192.168.73.0/24
Mobile VPN Client	192.168.100.1

Firewall A

External Interface	199.120.225.71/24
Local Network A	192.168.71.0/24

Create the VPN configuration on Firewall A.

1. Address object which contains the supernetted address for the entire network. In our example this would be 192.168.0.0/16
2. VPN object that references Firewall A's local network.
3. VPN authorization (policy) that references the address object created in step #1.
4. Remote Access filters to allow ESP and IKE connections to and from the transit point.
5. IP Pass Through Filters to control access to and from local network of A to HUB and additional networks. .

Address Objects

1 **Corporate_WAN** – Supernetted object containing company networks and mobile clients.
192.168.0.0/16

2 **Protected Networks** – Contains Firewall A's local network.
192.168.71.0/24

VPN Objects

1 IKE VPNs

	Name	IKE-HUB
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Protected Networks
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	AES-128
	Hash	hmac-sha1
	Key Group	group 2

Phase 1 and Phase 2 must match the transit point's VPN object definition.

VPNs Authorization

This VPN policy references the VPN Object **IKE – HUB** and the Address Object Corporate_WAN which contains the suppernetted addresses for the entire corporate WAN/LAN.

1 Firewall A to Transit Point (HUB)

Key exchange	IKE
VPN object	IKE-HUB
Remote network	Corporate _ WAN
Remote gateway	199.120.225.73
SAs	2

Remote Access Filters

Allow ESP connections from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	50
Source IP	199.120.225.73/32
Destination IP	EXTERNAL

Allow access to IKE from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	UDP
Source IP	199.120.225.73/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

These are the same filters as on Firewall B.

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from HUB and remote networks.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	Corporate _ WAN
Destination IP	Protected Networks Object

Allow outbound to HUB and remote networks.

Type	Accept
Interface	Protected
Protocol	ANY
Source IP	Protected Networks Object
Destination IP	Corporate _ WAN

Firewall B

External Interface	199.120.225.72/24
Local Network B	192.168.72.0/24

Create the VPN configuration on Firewall B.

1. Address object which contains the supernetted address for the entire network. In our example this would be 192.168.0.0/16
2. VPN object that references Firewall B's local network.
3. VPN authorization (policy) that references the address object created in step #1.
4. Remote Access filters to allow ESP and IKE connections to and from the transit point.
5. IP Pass Through Filters to control access to and from local network of B to HUB and additional networks.

Address Objects

1 Corporate_WAN.Supernetted Object containing all networks in the company. 192.168.0.0/16

2 Protected Networks – contains B's local network. 192.168.72.0/24

VPN Objects

1 IKE VPNs

	Name	IKE-HUB
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Protected Networks
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	AES-128
	Hash	hmac-sha1
	Key Group	group 2

VPNs Authorization

This VPN policy references the VPN Object **IKE – HUB** and the Address Object Corporate_WAN which contains all IP addresses for the corporate LAN.

1 Firewall B to HUB

Key exchange	IKE
VPN object	IKE-HUB
Remote network	Corporate _ WAN
Remote gateway	199.120.225.73
SAs	2

Remote Access Filters

Allow ESP connections from VPN transit point (HUB)

Type	Accept
Interface	EXTERNAL
Protocol	50
Source IP	199.120.225.73/32
Destination IP	EXTERNAL

Allow connections for IKE from VPN transit point (HUB)

Type	Accept
Interface	EXTERNAL
Protocol	UDP
Source IP	199.120.225.73/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

These are the same filters as on Firewall A.

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from transit point (HUB) and remote networks.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	Corporate _ WAN
Destination IP	Protected Networks Object

Allow outbound from Firewall B's local network to transit point (HUB) and remote networks.

Type	Accept
Interface	Protected
Protocol	ANY
Source IP	Protected Networks Object
Destination IP	Corporate _ WAN

Firewall Hub

External Interface	199.120.225.73/24
Local Network Hub	192.168.73.0/24

Create the VPN configuration at the transit point.

1. Address object which contains the supernetted address for the entire network. In our example this would be 192.168.0.0/16

2. Address Object for the A network.

3. Address Object that the B network.

4. VPN object that references the Address Object created in step 1.

5. Mobile VPN Object that references Address Object created in step 1.

6. VPN Authorization (policy) that references the address object created for the A network, and references the VPN Object created in step 4.

7. VPN Authorization (policy) that references the address object created for the B network, and references the VPN Object created in step 4.

8. Mobile User that references the Mobile VPN object created in step 5.
9. Remote Access filters to allow ESP and IKE connections. Since Mobile clients are involved these can be broad filters. If no mobile clients are in the configuration the filters can be specific to the remote firewalls establishing the VPN.
10. IP Pass Through filters to control access to and from the local networks and the VPN client.

Address Objects

1 **Corporate_WAN** – .Supernetted Object containing all networks in the company and Mobile clients.
192.168.0.0/16

2. **Mobile User** – Virtual IP assigned to mobile VPN client.
192.168.100.1
3. **A-Network** – Local network behind firewall A

   192.168.71.0/24
4. **B-Network** – Local network behind firewall B.
192.168.72.0/24

VPN Objects

1 IKE VPNs

	Name	IKE-HUB
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Corporate_WAN
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	AES-128
	Hash	hmac-sha1
	Key Group	group 2

2. Mobile VPNs

	Name	Mobile
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Corporate_WAN
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	3DES
	Hash	hmac-sha1
	Key Group	group 2

VPNs Authorization

1 From Firewall A to transit point (HUB)

Key exchange	IKE
VPN object	IKE-HUB
Remote network	A-Network
Remote gateway	199.120.225.71
SAs	2

2 From Firewall B to transit point (HUB)

Key exchange	IKE
VPN object	IKE-HUB
Remote network	B-Network
Remote gateway	199.120.225.72
SAs	2

Users Authorization

Name	Technical Support
Description	Support Group
Identity	support@gta.com
Auth method	password
VPN object	MOBILE
Remote network	192.168.100.1
Security associations	2

Remote Access Filters

Allow ESP connections from Mobile Clients and Remote Firewalls

Type	Accept
Interface	ANY
Protocol	50
Source IP	ANY_IP
Destination IP	EXTERNAL

Allow IKE connections from Mobile Clients and Remote Firewalls

Type	Accept
Interface	ANY
Protocol	UDP
Source IP	ANY_IP
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from A-Network to transit point (HUB) and remote networks.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	A-Network
Destination IP	Corporate_WAN

Allow outbound from transit point (HUB) and remote networks to A-Network

Type	Accept
Interface	Protected
Protocol	ANY
Source IP	Corporate_WAN
Destination IP	A-Network Object

Allow outbound from transit point (HUB), and remote networks to the VPN clients

Type	Accept
Interface	Protected
Protocol	ANY
Source IP	Corporate_WAN
Destination IP	192.168.100.0/24

Allow inbound from B-Network to transit point (HUB) and remote networks.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	B-Network Object
Destination IP	Corporate_WAN

Allow inbound from Mobile Clients to HUB and remote networks.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	192.168.100.0/24
Destination IP	Corporate_WAN

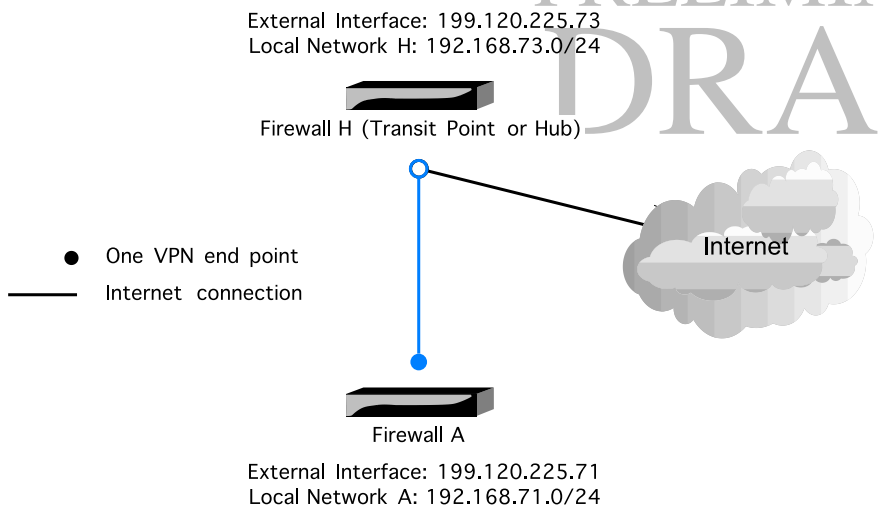
Allow outbound from transit point (HUB) and remote networks to B-Network

Type	Accept
Interface	Protected
Protocol	ANY
Source IP	Corporate_WAN
Destination IP	B-Network Object

Mobile VPN Client Configuration

The VPN client will follow the standard configuration outlined in the VPN documentation **GNAT Box VPN and VPN Client Feature Guide,** found at *at www.gta.com/support2/documents/.*

Note that the mobile VPN client has only one policy configured. This points to the External interface of the HUB as the gateway to the 192.168.0.0/16. All three remote networks (192.168.71.0 – 192.168.73.255) are encompassed in the supernetted network IP address.



Centralized Internet Access Management using VPNs:

GNAT Box System Software version 3.5 and above

The following example illustrates how to configure centralized Internet access management using VPNs to provide access for a remote firewall. To use this configuration, the transit point firewall must be on GNAT Box System Software version 3.5.x. and GTA recommends that all firewalls be on the same version.

For best performance, GTA recommends a GB-1500 for the transit point firewall.

Before implementing this configuration, consider:

- Number of users at remote sites and HUB.
- Types of Internet access allowed.
- Bandwidth at the transit point.
- Firewall capabilities at the transit point.

IP Pass Through filters shown in the example allow all access. Consult your corporate security policy for access restrictions through the established VPN.

IP Addresses

```
Firewall HUB   199.120.225.73/24
 Network HUB   192.168.73.0/24

 Firewall A    199.120.225.71/24
  Network A    192.168.71.0/24
```

Firewall A

```
External Interface 199.120.225.71/24

Local Network A    192.168.71.0/24
```

Create the VPN configuration on Firewall A.

1. VPN object that references Firewall A's local network.
2. VPN authorization that references 0.0.0.0/0.
3. Remote Access filters to allow ESP and IKE connections from the transit point/HUB.
4. IP Pass Through Filters to control access to the transit point and the Internet.

Address Objects

Protected Networks – Contains Firewall A's local network.
192.168.71.0/24

VPN Objects

1 IKE VPNs

```
              Name  IKE-HUB
    Authentication  no
           Gateway  EXTERNAL
       Force mobile  no
     Local network  Protected Networks
Phase 1       Mode  main
               ESP  3des
              Hash  hmac-sha1
         Key Group  group 2
Phase 2        ESP  AES-128
              Hash  hmac-sha1
         Key Group  group 2
```

Phase 1 and Phase 2 must match the transit point's VPN object definition.

VPNs Authorization

Firewall A to Transit Point (HUB)

```
      Key exchange  IKE
        VPN object  IKE-HUB
    Remote network  0.0.0.0/0
    Remote gateway  199.120.225.73
               SAs  2
```

Remote Access Filters

Allow ESP connections from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	50
Source IP	199.120.225.73/32
Destination IP	EXTERNAL

Allow access to IKE from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	UDP
Source IP	199.120.225.73/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from HUB and Internet through VPN.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	ANY_IP
Destination IP	Protected Networks Object

Allow outbound to HUB and Internet.

Type	Accept
Interface	PROTECTED
Protocol	ANY
Source IP	Protected Networks Object
Destination IP	ANY_IP

Firewall Hub

External Interface	199.120.225.73/24
Local Network Hub	192.168.73.0/24

Create the VPN configuration at the transit point.

1. Address Object for the A network.
2. VPN Object which references 0.0.0.0/0
3. VPN policy that references the object created in step 2 and a remote network of Firewall A.
4. IP Pass Through Filters to control access to the local network and the Internet.

Address Objects

A-Network – Local network behind firewall A
192.168.71.0/24

VPN Objects

IKE VPNs

Name	IKE-HUB
Authentication	no
Gateway	EXTERNAL
Force mobile	no
Local network	0.0.0.0/0
Phase 1 Mode	main
ESP	3des
Hash	hmac-sha1
Key Group	group 2
Phase 2 ESP	AES-128
Hash	hmac-sha1
Key Group	group 2

VPNs Authorization

From Firewall A to transit point (HUB)

Key exchange	IKE
VPN object	IKE-HUB
Remote network	A-Network
Remote gateway	199.120.225.71
SAs	2

Remote Access Filters

Allow ESP connections from Remote Firewalls

Type	Accept
Interface	ANY
Protocol	50
Source IP	199.120.225.71/32
Destination IP	EXTERNAL

Allow IKE connections from Remote Firewalls

Type	Accept
Interface	ANY
Protocol	UDP
Source IP	199.120.225.71/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

IP Pass Through Filters

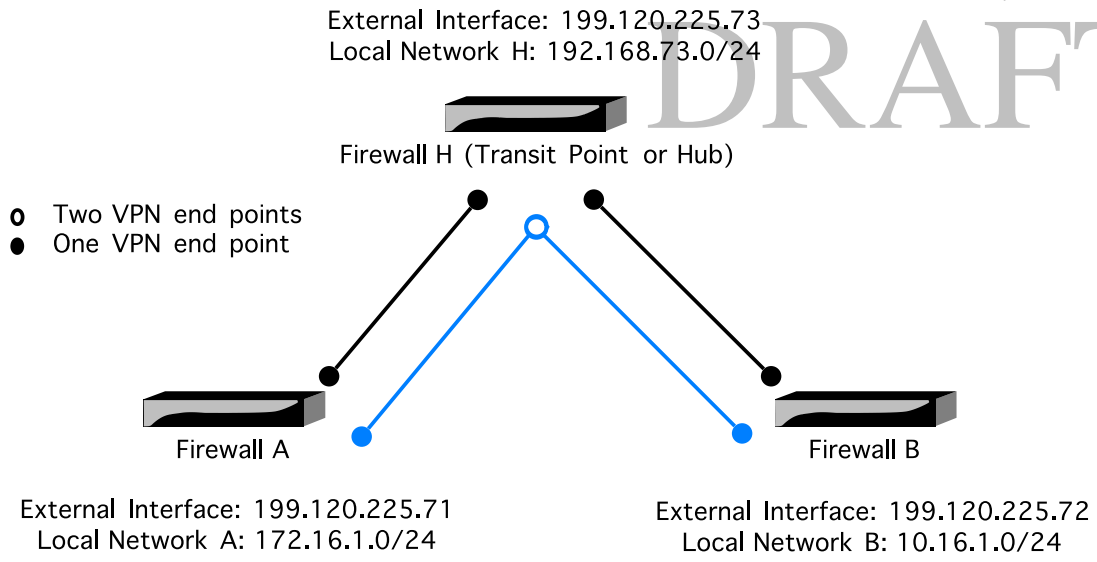
IP Pass Through filters shown allow all access.

Allow inbound from A-Network to transit point/HUB and the Internet.

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	A-Network
Destination IP	ANY_IP

Allow outbound Internet traffic and transit point/HUB to A-Network

Type	Accept
Interface	PROTECTED
Protocol	ANY
Source IP	ANY_IP
Destination IP	A-Network Object



Fully connected three-network VPN configuration using a hub

Fully connect three separate networks

with a Transit Point (hub/spoke) VPN

This example demonstrates how to configure VPNs for a fully connected three-network using a transit point/hub, in an environment where supernetting cannot be used.

IP Addresses

```
Firewall A   199.120.225.71
 Network A   172.16.1.0/24
Firewall B   199.120.225.72
 Network B   10.1.16.0/24
Firewall H   199.120.225.73
 Network H   192.168.73.0/24
```

Firewall A

```
External Interface     199.120.225.71/24
Local Network A        172.16.1.0/24
```

Create the VPN configuration on Firewall A.

1. Address object which contains the transit point's local network and Firewall B's local network.
2. VPN object that references Firewall A's local network.
3. VPN authorization (policy) that references the address object created in step #1.
4. Remote Access filters to allow ESP and IKE connections to and from the transit point.
5. IP Pass Through Filters to control access to and from Firewall A's local network to the transit point (HUB) and to B.

Address Objects

1 **HUB & B** – Includes transit point's local network and B's local network.
10.1.16.0/24
192.168.73.0/24

2 **Protected Networks** – Contains A's local network.
172.16.1.0/24

VPN Objects

Phase 1 and Phase 2 must match the transit point's VPN object definition.

1 IKE VPNs

```
                Name  IKE-HUB
      Authentication  no
             Gateway  EXTERNAL
       Force mobile   no
      Local network   Protected Networks
Phase 1        Mode   main
                ESP   3des
               Hash   hmac-sha1
          Key Group   group 2
Phase 2         ESP   3des
               Hash   hmac-sha1
          Key Group   group 2
```

VPNs Authorization

This VPN policy references the VPN Object **IKE – HUB** and the Address Object **HUB & B** which contain the transit point's local network and Firewall B's local network.

1 Firewall A to Transit Point (HUB)

Key exchange	IKE
VPN object	IKE-HUB
Remote network	HUB & B
Remote gateway	199.120.225.73
SAs	4

Remote Access Filters

Allow ESP connections from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	50
Source IP	199.120.225.73/32
Destination IP	EXTERNAL

Allow access to IKE from transit point (HUB)

Type	Accept
Interface	ANY
Protocol	UDP
Source IP	199.120.225.73/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

These are the same filters as on Firewall B.

IP Pass Through Filters

IP Pass Through filters shown allow all access. Consult your corporate security policy for access restrictions through the established VPN.

Allow inbound from HUB & B

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	HUB & B Object
Destination IP	Protected Networks Object

Allow outbound to HUB & B

Type	Accept
Interface	PROTECTED
Protocol	ANY
Source IP	Protected Networks Object
Destination IP	HUB & B Object

Firewall B

External Interface	199.120.225.72/24
Local Network B	10.1.16.0/24

Create the VPN configuration on Firewall B.

1. Address object which contains the transit point (HUB) local network and Firewall A's local network.
2. VPN object that references the local network for Firewall B.
3. VPN authorization (policy) that references the address object created in step #1.
4. Remote Access filters to allow ESP and IKE connections to and from the Transit Point (HUB).
5. IP Pass Through Filters to control access to and from local network of B to the transit point (HUB) and to A.

Address Objects

1 HUB & A – includes hub's local network and A's local network.
172.16.1.0/24
192.168.73.0/24

2 Protected Networks – contains B's local network.
10.1.16.0/24

VPN Objects

1 IKE VPNs

	Name	IKE-HUB
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Protected Networks
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2

VPNs Authorization

This VPN policy references the VPN Object **IKE – HUB** and the Address Object **HUB & A** which contain the transit point's local network and Firewall A's local network.

1 Firewall B to Hub

Key exchange	IKE
VPN object	IKE-HUB
Remote network	HUB & A
Remote gateway	199.120.225.73
SAs	4

Remote Access Filters

Allow ESP connections from VPN transit point (HUB)

Type	Accept
Interface	EXTERNAL
Protocol	50
Source IP	199.120.225.73/32
Destination IP	EXTERNAL

Allow IKE connections from VPN transit point (HUB)

Type	Accept
Interface	EXTERNAL
Protocol	UDP
Source IP	199.120.225.73/32
Source Port	500 or blank
Destination IP	EXTERNAL
Destination Port	500

These are the same filters as on Firewall A.

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from transit point (HUB) and Firewall A's local networks to Firewall B's local network

Type	Accept
Interface	EXTERNAL
Protocol	ANY
Source IP	HUB & A Object
Destination IP	Protected Networks Object

Allow outbound from Firewall B's local network to transit point (HUB) and Firewall A's local networks

Type	Accept
Interface	PROTECTED
Protocol	ANY
Source IP	Protected Networks Object
Destination IP	HUB & A Object

Firewall Hub

External Interface	199.120.225.73/24
Local Network Hub	192.168.73.0/24

Create the VPN configuration at the transit point.

1. Address objects which contain the following:
   - HUB's local network and A's local network.
   - HUB's local network and B's local network.
   - A's Local network.
   - B's local network.
2. VPN object that references HUB & A's local network.
3. VPN object that references HUB & B's local network.
4. VPN Authorization (policy) that references Firewall A's address object created in step #1.
5. VPN Authorization (policy) that references Firewall B's address object created in step #1.
6. Remote Access filters to allow ESP and IKE connections from Firewalls A and B.
7. IP Pass Through filters to control access to and from the local networks of A to the HUB and to B, and the local networks of B to the HUB and A.

Address Objects

1 HUB & A – local networks for Transit Point (HUB) and A.
172.16.1.0/24
192.168.73.0/24

2 HUB & B – local networks for Transit Point (HUB) and B.
10.1.16.0/24
192.168.73.0/24

3 A-Network – Local network for Firewall A.
172.16.1.0/24

4 B-Network – Local network for Firewall B.
10.1.16.0/24

VPN Objects

1 IKE VPNs

	Name	IKE-HUB-A
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	HUB & A
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2

2 IKE VPNs

	Name	IKE-HUB-B
	Authentication	no
	Gateway	EXTERNAL
	Force mobile	no
	Local network	Hub & B
Phase 1	Mode	main
	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2
Phase 2	ESP	3des
	Hash	hmac-sha1
	Key Group	group 2

VPNs Authorization

1 From Firewall A to transit point (HUB) and B

```
Key exchange  IKE
  VPN object  IKE-HUB-B
Remote network  A-Network
Remote gateway  199.120.225.71
         SAs  4
```

2 From Firewall B to transit point (HUB) and A

```
Key exchange  IKE
  VPN object  IKE-HUB-A
Remote network  B-Network
Remote gateway  199.120.225.72
         SAs  4
```

Remote Access Filters

Allow ESP connections from Firewall A

```
          Type  Accept
     Interface  ANY
      Protocol  50
     Source IP  199.120.225.71/32
Destination IP  EXTERNAL
```

Allow IKE connections from Firewall A

```
          Type  Accept
     Interface  ANY
      Protocol  UDP
     Source IP  199.120.225.71/32
   Source Port  500 or blank
Destination IP  EXTERNAL
Destination Port  500
```

Allow ESP connections from Firewall B

```
          Type  Accept
     Interface  ANY
      Protocol  50
     Source IP  199.120.225.72/32
Destination IP  EXTERNAL
```

Allow IKE connections from Firewall B

```
          Type  Accept
     Interface  ANY
      Protocol  UDP
     Source IP  199.120.225.72/32
   Source Port  500 or blank
Destination IP  EXTERNAL
Destination Port  500
```

IP Pass Through Filters

IP Pass Through filters shown allow all access.

Allow inbound from A-Network to transit point (HUB) and B-Network

```
          Type  Accept
     Interface  EXTERNAL
      Protocol  ANY
     Source IP  A-Network
Destination IP  HUB & B Object
```

Allow outbound from transit point (HUB) and B-Network to A-Network

```
          Type  Accept
     Interface  PROTECTED
      Protocol  ANY
     Source IP  HUB & B Object
Destination IP  A-Network Object
```

Allow inbound from B-Network to transit point (HUB) and A-Network

```
          Type  Accept
     Interface  EXTERNAL
      Protocol  ANY
     Source IP  B-Network Object
Destination IP  HUB & A Object
```

Allow outbound from transit point (HUB) and B-Network to A-Network

```
          Type  Accept
     Interface  PROTECTED
      Protocol  ANY
     Source IP  HUB & A Object
Destination IP  B-Network Object
```


Global Technology Associates, Inc.

3505 Lake Lynda Drive, Suite 109 • Orlando, FL 32817 USA

Tel: +1.407.380.0220 • Fax: +1.407.380.6080 • Web: http://www.gta.com • Email: info@gta.com