High Availability Branch Office VPN

J Wolfgang Goerlich
Written October 2007

Business Objective

A business has a main office and a branch office. These are to be connected by an IPSEC site-to-site VPN tunnel. Availability is the key design factor. Connectivity from the branch office to the main office must continue in the face of multiple failures.

This whitepaper details an example of such a highly available VPN tunnel. It then walks the reader thru setting up such a tunnel in a lab environment.

Creative Commons Copyright and Use Notice

Table of Contents

Introduction

With firmware 9x, WatchGuard has added high availability to its Firebox Peak series firewalls. High availability (HA) allows two Fireboxes to be setup in an active-passive configuration. Should the active Firebox lose connectivity or have a hardware failure, the passive Firebox takes over. Generally this happens so quickly as to not interrupt any communications. Even latency sensitive applications such as Terminal Services will not be interrupted during a HA fail-over.

Network Design

Figure 1 shows a redundant office connection. This same design would be used in the main office and in any future branch offices.

First, use two Firebox X6500e devices with HA enabled. Both will be powered up. The primary will handle all network traffic and serve as the VPN end-point. The secondary will be on standby. The secondary only becomes active in the event of a fail-over. At that time, it will assume the IP and MAC addresses of the primary and resume connectivity.

Second, use two Internet connections. To minimize the chances of a single point of failure, ensure that these come from two different Internet Service Providers (ISP). Check with the ISPs and make certain that they use different routes out to the Internet backbone. When running the circuit into the office, use a separate demarc. Each demarc should also be on a separate power circuit.

Third, connect the Fireboxes to the Internet by way of two Cisco 2800 Series routers. There will be two Firebox connections to each router. Since this is active-passive, however, only one interface will have an active MAC and IP address during normal operations. Place the two Cisco routers on separate power circuits as well.

There are two single point of failure in this model. The first is primary AC, which can be mitigated with a UPS or a generator. The second is the Ethernet switch.

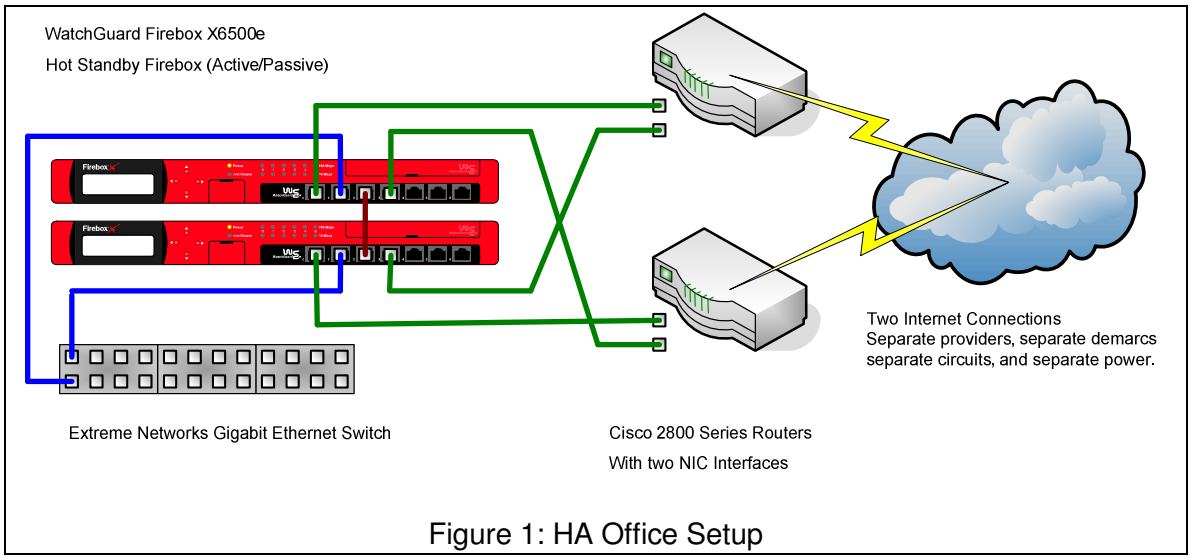

Figure 1: HA Office Setup

High Availability Lab Setup

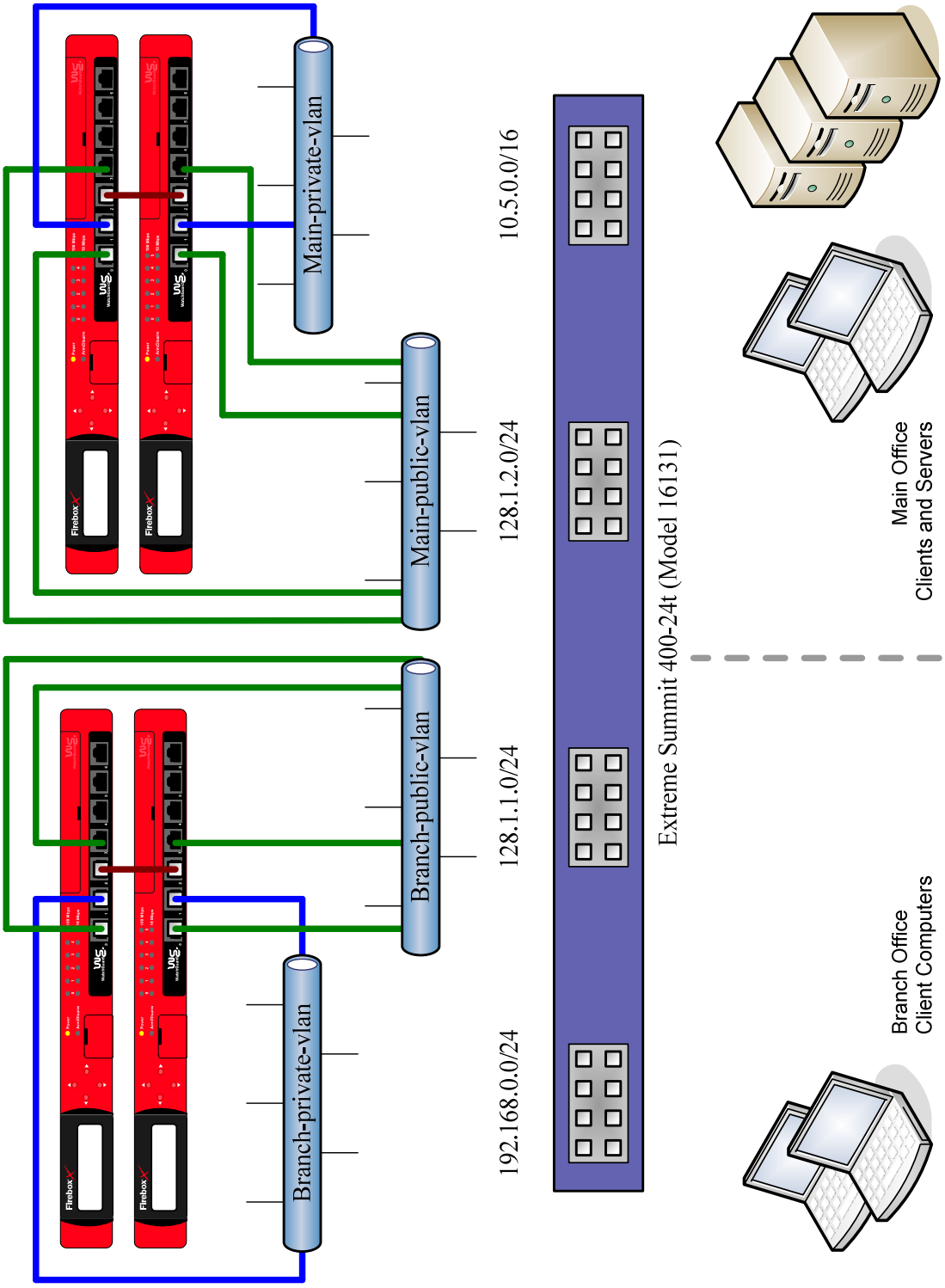

Figure 2: HA Lab Setup

Details

Extreme Switch Management IP	10.5.0.2/16
Branch Office Network Vlan	Branch-private-vlan
Branch Office Vlan Ports	1-8
Branch Office Network	192.168.0.0/24
Branch Office DHCP Scope	192.168.0.20-192.168.0.200
Branch Office Internet Vlan	Branch-public-vlan
Branch Office Vlan Ports	9-12
Branch Office Internet	128.1.1.0/24
Branch Office Internet Gateway	128.1.1.1
Branch Office Firebox Trusted	192.168.0.1
Branch Office Firebox External	128.1.1.2
Branch Office Firebox Optional	128.1.1.3
Main Office Network Vlan	Main-private-vlan
Main Office Vlan Ports	17-24
Main Office Network	10.5.0.0/16
Main Office Internet Vlan	Main-public-vlan
Main Office Vlan Ports	13-16
Main Office Internet	128.1.2.0/24
Main Office Internet Gateway	128.1.2.1
Main Office Firebox Trusted	10.5.0.1
Main Office Firebox External	128.1.2.2
Main Office Firebox Optional	128.1.2.3
Primary Branch Office Firewall	Bo1
Primary Branch Office Trusted Port	1
Primary Branch Office Optional Port	9
Primary Branch Office External Port	10
Secondary Branch Office Firewall	Bo2
Secondary Branch Office Trusted Port	2
Secondary Branch Office Optional Port	11
Secondary Branch Office External Port	12
Primary Main Office Firewall	Mo1
Primary Main Office Trusted Port	17
Primary Main Office Optional Port	13
Primary Main Office External Port	14
Secondary Main Office Firewall	Mo2
Secondary Main Office Trusted Port	18
Secondary Main Office Optional Port	15
Secondary Main Office External Port	16

Main Office Active Directory Controller	10.5.0.48/16
Active Directory Domain	Dualoffice.test

Extreme Summit 400-24t (Model 16131)

1	3	5	7	9	11	13	15	17	19	21	23
2	4	6	8	10	12	14	16	18	20	22	24

Setup the Main Office

The example main office will have a domain controller, a file server, and a Windows Terminal Server. These should be in a single Active Directory domain.

Connect these into the [Main Office Vlan Ports] on the switch. Give them static IP addresses from the [Main Office Network] range. Use the [Main Office Firebox Trusted] address for the default gateway. Note that all devices that participate in the VPN must use the Firebox as their gateway in order for the tunnel to route traffic across.

Build a Windows 2003 Active Directory domain controller with the IP address specified in [Main Office Active Directory Controller]. Install DNS and WINS on this computer.

Build a Windows 2003 file server. Join it to the domain.

Build a Windows 2003 Terminal Server. Install Microsoft Office 2003.

Get all of the main office servers up to the latest updates and patch levels.

Setup an Enterprise Certification Authority

Install and configure a enterprise CA (certification authority) on the [Main Office Active Directory Controller] computer.

Planning the installation of a certification authority
http://technet2.microsoft.com/windowsserver/en/library/d6eab6a4-a680-40b0-9fde-4978be14ebf41033.mspx?mfr=true

Setup the Management Station

Select a computer to be the management station. On a computer, install the Fireware firmware, WatchGuard System Manager and System Management Server. Also download the manuals.

WatchGuard Fireware OS Fireware91.exe
WatchGuard System Manager WSM91s.exe
WatchGuard Quick Start Guide ..... quickstartguide_eseries.pdf
WatchGuard User Guide v91wsmuserguide.pdf

Setup the management server on this computer.

Activate the fireboxes

Follow the Quick Start Guide. Install software on your Firebox.

C:\Program Files\Common Files\WatchGuard\resources\Fireware\9.1\fbx_ta-9.1-b20030.wgf

[ ] Allow this Firebox to be managed by a remote computer

Configure the name, external interface, optional interface according to the information above.

[x] I would like to manually configure the DNS information for my Firebox.
Domain Name: [Active Directory Domain]
DNS Servers: [Main Office Active Directory Controller]

Setup the Fireboxes to be managed

On the management station: install the WatchGuard System Management server. Create entries in your Hosts file, mapping the trusted IP addresses to the Fireboxes FQDN; for example, Fw1.mydomain.local.

Currently, all four boxes are on the same network segment (or Vlan). After we have registered the Fireboxes with the management station, we will create separate Vlans to simulate the offices and Internet connection.

Bind an IP address on the management station for both subnets. Ping all three trusted internal interfaces from the management station. Make sure you can ping before proceeding.

Add the devices to the WatchGuard System Manager > Management Server
Select the default method to authenticate IPSec tunnels with this device

(o) Firebox Certificate (RSA Signature)

IMPORTANT: The serial number must be displayed under Device Information in System Manager.

Reconfigure all devices in the WatchGuard System Manager > Management Server. Add the Trusted Interface IP address to the list (it changes to the external interface when importing). Click Update Device and check [x] Reset server configuration and [x] Issue/Reissue Firebox's IPSec Certificate.

Follow the steps in the WatchGuard User Guide, "Certificates and the Certificate Authority", page 349.

Name: (Name of the Firebox, example: Fw1)
Department: Infrastructure
Company: My Test Biz
City:
State:
Country:

Subject name: (auto generated)
DNS name: (FQDN of the Firebox, example: Fw1.mydomain.local)
IP Address: [Branch Office Firebox External] or appropriate firewall
User Domain Name: (your email address)

(o) RSA
(o) 1024
(o) Both

Save each request down as a file.

- [Primary Branch Office Firewall].txt
- [Secondary Branch Office Firewall].txt
- [Primary Main Office Firewall].txt

- [Secondary Main Office Firewall].txt

Save these files off onto the CA [Main Office Active Directory Controller]. Fulfill the requests and generate the certificates. Use the Certificate Template: IPSec (Offline Request) and save as Base-64 cert files. Also, export the root CA certificate.

- [Primary Branch Office Firewall].cer
- [Secondary Branch Office Firewall].cer
- [Primary Main Office Firewall].cer
- [Secondary Main Office Firewall].cer
- CA.cer

On the firewalls, import the CA Certificate. Then, import the newly created firewall certificates.

Note that if (a) the CA certificate is not installed; or (b) the WatchGuard System Manager (WSM) does not read the Firebox's serial number, the following error may occur:

Error Code: 2023:40B2
Error Message: Error (16562), serial number not found in database

Ensure that the certificates listed show the new certificate as signed. Then, reboot the Fireboxes from the System Manager.

Set the time

For each Firebox, open Policy Manager and set the time zone. Save back to the Firebox.

Open System Manager. Synchronize with the management station.

Setup WINS and DNS

Right-click the Fireboxes, Properties
IPSec Tunnel Preferences
Tunnel authentication: IPSec Firebox Certificate
WINS Primary: [Main Office Active Directory Controller]
WINS Secondary: (blank)
DNS Primary: [Main Office Active Directory Controller]
DNS Secondary: (blank)
Domain suffix: [Active Directory Domain]

Create a Managed Site-to-Site VPN

All four Fireboxes must be accessible from the management station for this next step. This may mean that they are all on the same network segment or Vlan. Or it may mean that the Vlans are routing between each other. If you are following this lab step-by-step, then the Fireboxes are currently on one Vlan but separate subnets.

Ping all four trusted internal interfaces from the management station. Make sure you can ping before proceeding.

Follow the steps in the WatchGuard User Guide, "Adding VPN Resources" on page 320.

On the [Primary Branch Office Firewall] firewall:
Add: Branch-Main Policy
Allow to/from: [Main Office Network]

On the [Primary Main Office Firewall] firewall:
Add: Main-Branch Policy
Allow to/from: [Branch Office Network]

Add networks:
[Main Office Network]
[Branch Office Network]

See "Adding VPN Firewall Policy Templates" on page 322.

Company-VPN-Policy
Any Protocol, Any Port
[ ] Enable logging for this traffic

See "Making Tunnels Between Devices" on page 325.

Drag [Primary Branch Office Firewall] to [Primary Main Office Firewall].

Device one:
Device: [Primary Branch Office Firewall]
VPN Resource: Branch-Main Policy

Device two:
Device: [Primary Main Office Firewall]
VPN Resource: Main-Branch Policy

Security Template: Strong with Authentication
[x] Use nameservers (DNS/WINS) from [Primary Main Office Firewall]

VPN Firewall Policy Template:
Company-VPN-Policy

[x] Restart the devices now to download VPN configuration

Now that all of the Fireboxes are managed and the managed VPN is in place, we can remove all four devices from being on the same vlan.

Setup the Management Interface (Optional)

Telnet into the Extreme switch directly over serial cable.

configure vlan [Branch Office Network Vlan] ipa [Extreme Switch Management IP] [Subnet mask in decimal]
enable ip
save primary

Note that in a real world scenario, the branch office and main office would be in two separate buildings and on two separate Ethernet switches. You may want to manage the branch office switch from the main office, or vice versus. To do so, set the default gateway on the switch to point to the Firebox trusted interface.

configure iproute add default [Branch Office Firebox Trusted]

Create the VLANs

Telnet [Extreme Switch Management IP]

create vlan [Branch Office Network Vlan]
show [Branch Office Network Vlan]

If the port is already in use, you will have to first remove it from the Vlan.
configure vlan [Vlan name] delete port [Port number]

Add the port into the Vlan.
configure vlan [Branch Office Network Vlan] add port [Port number]

Confirm that the ports were added and then save.
show [Branch Office Network Vlan]
save primary

Repeat the above steps to create [Branch Office Internet Vlan], [Main Office Internet Vlan], and [Main Office Network Vlan].

Enable Routing to Simulate Internet

We will setup an IP address as a gateway. Then, we enable routing between the two “Internet” Vlans. This simulates a route path, like the Internet, and is important in getting the two VPN tunnels to work.

configure [Branch Office Internet Vlan] ipaddress [Branch Office Internet Gateway]/[Subnet mask]
configure [Main Office Internet Vlan] ipaddress [Main Office Internet Gateway]/[Subnet mask]
enable ipforward
save primary

Enable DHCP

The DHCP server that comes with the Extreme switch is rather limited and not recommended for highly utilized environments. We cannot use the WatchGuard Firebox DHCP, however, as it is disabled when HA (high availability) is on.

configure vlan [Branch Office Network Vlan] dhcp-address-range [Branch Office DHCP Scope]
configure vlan [Branch Office Network Vlan] dhcp-options dns-server 110.50.1.48
configure vlan [Branch Office Network Vlan] dhcp-options dns-server 110.50.1.49
configure vlan [Branch Office Network Vlan] dhcp-options wins-server 110.50.1.252
configure vlan [Branch Office Network Vlan] dhcp-options wins-server 110.50.1.253
configure vlan [Branch Office Network Vlan] dhcp-options default-gateway 192.168.0.3
save primary

Setup the secondary Internet connection

Open Policy Manager on [Primary Branch Office Firewall]. Open Network > Configuration. Modify Optional-1.

Policy Manager
Modify Optional-1

Interface name (Alias): Optional-1
Interface description: Redundant Internet Link
Interface type: External

(o) Use Static IP
IP Address: [Branch Office Firebox Optional]
Default Gateway: [Branch Office Internet Gateway]

Repeat this process for the [Primary Main Office Firewall]. For additional information, see WatchGuard User Guide, “About VPN Failover” on page 344.

Create a Manual Site-to-Site VPN

Open Policy Manager on [Primary Main Office Firewall]. Open VPN > Branch Office Gateways.

Add:
Gateway name: Branch
(o) Use IPSec Firebox Certificate

Gateway Endpoints, Add:

Local Gateway:
(o) By Domain Information, [Configure], (o) By x500 Name
External interface: External

Remote Gateway
(o) Static IP address: [Branch Office Firebox External]
(o) By Domain Information, [Configure], (o) By x500 Name

Remote Gateway
(o) Static IP address: [Branch Office Firebox Optional]
(o) By Domain Information, [Configure], (o) By x500 Name

Open Policy Manager on [Primary Main Office Firewall]. Open VPN > Branch Office Tunnels.

Add:
Tunnel Name: Main-Branch Tunnel

Add networks:
Local: [Main Office Network]
Remote: [Branch Office Network]
Direction: <===>

[x] Add this tunnel to the BOVPN-Allow policies

Now repeat this process on the other side of the tunnel. Open Policy Manager on [Branch Main Office Firewall]. Open VPN > Branch Office Gateways.

Add:
Gateway name: Main
(o) Use IPSec Firebox Certificate

Gateway Endpoints, Add:

Local Gateway:
(o) By Domain Information, [Configure], (o) By x500 Name
External interface: External

Remote Gateway
(o) Static IP address: [Main Office Firebox External]
(o) By Domain Information, [Configure], (o) By x500 Name

Remote Gateway
(o) Static IP address: [Main Office Firebox Optional]
(o) By Domain Information, [Configure], (o) By x500 Name

Open Policy Manager on [Primary Branch Office Firewall]. Open VPN > Branch Office Tunnels.

Add:
Tunnel Name: Branch-Main Tunnel

Add networks:
Local: [Branch Office Network]
Remote: [Main Office Network]
Direction: <===>

[x] Add this tunnel to the BOVPN-Allow policies

Setup High Availability

You must use DHCP from a different device than the Firebox. If you attempt to enable HA and DHCP, the following event occurs:

Fireware Policy Manager
Can't enable High Availability because the Trusted Interface, Trusted, is configured to use DHCP server.

Turn off [Secondary Branch Office Firewall] and [Secondary Main Office Firewall].

[Primary Branch Office Firewall] port 3 to [Secondary Branch Office Firewall] port 3 via a cross-over cable. Do the same for [Primary Main Office Firewall] and [Secondary Main Office Firewall].

Repeat this process for the [Primary Main Office Firewall].

Follow the steps in the WatchGuard User Guide, “High Availability” on page 461.

Testing

Try the following tests:

- ICMP
  - Ping across the VPN
  - Simulate a failure
    - Power off one of the Fireboxes (or)
    - Disconnect one of the Fireboxes' network cables
  - What happens to the ping response times during fail-over?
- CIFS
  - Start a file copy from the branch office client to the main office server
  - Simulate a failure
  - What happens to the file copy during a fail-over?
- RDP
  - Start an RDP session from the branch office client to the main office Terminal Server
  - Simulate a failure
  - What happens to the RDP session during fail-over?

Conclusions

WatchGuard's HA feature is another way to increase redundancy and fault-tolerance in site-to-site VPN designs. When coupled with other best practices, such as duplicate Internet connections and redundant power, true high availability becomes practical. The common network services – like file and print, terminal services – can continue uninterrupted in the face of multiple failures. This is an excellent design for when costs are second to up-time.