pfSense OpenVPN server with DD-WRT clients December 1, 2012 Tags: ddwrt, pfsense, router, vpn

Today’s task is a pfSense OpenVPN server with multiple routed site-to-site DD-WRT clients. Everything is done via web GUI to make setup as painless as possible. (;

Requirements: -one pfSense server -one or more DD-WRT routers with OpenVPN

1. Reset pfSense and DD-WRT to factory defaults.

2. Setup your LAN, WAN, DNS. Leave timezone as UTC for now.

Server Setup

3. System ⇒ Cert Manager ⇒ add new CA Descriptive name: YourCompanyVPNca Method: Create an internal Certificate Authority Key length: 2048 Lifetime: 3650 Common Name: vpn.yourdomain.com Fill in your information. Set common name to server’s FQDN.

Failure to use a FQDN common name is a cause of TLS errors while connecting. The error below is what happens if I do not use a FQDN. TLS Error: TLS handshake failed TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)

4. System ⇒ Cert Manager ⇒ Certificates ⇒ add new Method: Create an internal Certificate Descriptive name: YourCompanyVPNserver Certificate authority: Select the one you created. Key length: 2048 Certificate Type: User Common Name: vpn.yourdomain.com Fill in your information. Set common name to server’s FQDN.

5. VPN ⇒ OpenVPN ⇒ add new

General information: Server Mode: Remote Access (SSL/TLS) Protocol: UDP Device Mode: tun Interface: WAN Local port: 1194 You can set this to a non-standard port for increased security. Make sure you set the correct port on the firewall and client!

Cryptographic Settings: TLS Authentication: uncheck Peer Certificate Authority: Select the one you created. Server Certificate: Select the one you created. DH Parameters Length: 1024 Encryption algorithm: BF-CBC (128-bit) Certificate Depth: one

Tunnel Settings: Tunnel Network: 10.0.8.0/24 You can set this to anything! Use a custom value for added compatibility while on the road. Example: 10.81.18.0/24 Redirect Gateway: uncheck Set this per client. Note: This will not work with automatic NAT. Instructions are provided at the end of the article to configure manual outbound NAT. Local Network: 192.168.1.1/24 Enter pfSense’s LAN CIDR range. Change the interface default! This subnet is the default for residential routers. This will cause conflict when connecting from a home network. Concurrent connections: 10 Depends how many clients will be connecting. Compression: check Type-of-Service: uncheck Inter-client communication: check Duplicate Connections: uncheck

Client Settings: Dynamic IP: check Important when roaming between cellular networks, Wifi networks, etc. Address Pool: check DNS Default Domain: uncheck DNS Servers: uncheck NTP Servers: uncheck NetBIOS Options: uncheck

Advanced configuration: Set your routes here. Below is a two client example. This will teach you how to setup any number of clients.

Mike’s LAN is 10.1.1.0/24 John’s LAN is 10.2.2.0/24

To allow proper client communication for our routed setup we need to acheive two goals. 1. Push appropriate routes to clients. Example: push “route 10.1.1.0 255.255.255.0″; push “route 10.2.2.0 255.255.255.0″ 2. Add appropriate routes to server. Example: route 10.1.1.0 255.255.255.0; route 10.2.2.0 255.255.255.0

Based on the above example the advanced setting would be: push “route 10.1.1.0 255.255.255.0″; route 10.1.1.0 255.255.255.0; push “route 10.2.2.0 255.255.255.0″; route 10.2.2.0 255.255.255.0

CLICK SAVE!!

Next we will generate certificates for our clients.

6. System ⇒ Cert Manager ⇒ Certificates ⇒ add new Method: Create an internal Certificate Descriptive name: Mike Smith Certificate authority: Select the one you created. Key length: 2048 Certificate Type: User Lifetime: 3650 Distinguished name: Common Name: mike.yourdomain.com It’s best to make this client specific. Set the common name to Mike’s FQDN. If you don’t know it, make it up, mike.yourdomain.com. It is important to remember the EXACT string for the next step.

REPEAT FOR EACH CLIENT. Set a unique common name for every client certificate.

7. VPN ⇒ OpenVPN ⇒ Client Specific Overrides ⇒ add new Two behaviors of the VPN will be set here. The first, redirect gateway, pushes “redirect-gateway def1″. This allows internet traffic to be securely relayed before unencrypted transmission. Read the instructions at the end of the article if you plan on using this. Secondly, iroute, which stops OpenVPN from pushing the VPN route for the client’s LAN to the client.

Common name: mike.yourdomain.com Redirect Gateway: enable if desired Advanced: iroute 10.1.1.0 255.255.255.0

Leave everything else unchecked and blank. For clarity I will review John’s client specific override below.

VPN ⇒ OpenVPN ⇒ Client Specific Overrides ⇒ add new Common name: john.yourdomain.com Redirect Gateway: enable if desired Advanced: iroute 10.2.2.0 255.255.255.0

Note: Skip setting the iroute for single users. Optionally, add iroutes to prevent access to subnets and add routes to give special access. To control access when redirect gateway is enabled use firewall rules.

8. Firewall ⇒ rules ⇒ WAN ⇒ add new Protocol: UDP Destination: Type: WAN address Destination port range: from: 1194 Destination port range: to: 1194 Description: Mike and Johns VPN

9. Firewall ⇒ rules ⇒ OpenVPN Protocol: any Description: allow all VPN traffic

Most people want all traffic allowed through. To control traffic set rules here.

Save. Apply.

Note: If you live in a negative timezone and use certificates immediately after generating you will get this error: “TLS Error: Unroutable control packet received from x.x.x.x:1194 (si=3 op=P_CONTROL_V1).” To correct this set the server and client’s timezone to UTC. You can change it back after N hours have elapsed.

Install the OpenVPN Client Export Utility now. It becomes a snap to configure road warriors, remote-access or client-to-gateway, by generating a ready to install package for Windows or Mac with client specific details. This can be done by going to System ⇒ Package Manager.

Client Setup

Site-to-site client instructions are based on DD-WRT router firmware.

Most of my routers are Asus RT-N16. A few are the good-old Linksys WRT54GL routers! The instructions are the same for all DD-WRT routers.

I don’t use packages in the big or mega versions. To save RAM and NVRAM I am using the OpenVPN version. I am using build 15943-snow on the RT-N16 because it includes TCP Vegas for congestion control. The recommended Broadcom build as of December 1, 2012, is 14929. For the RT-N16 this can be downloaded here. For the WRT54GL this can be downloaded here.

Setting up DD-WRT requires downloading some certificates and a key from pfSense, pasting them into a script, pasting the script into DD-WRT’s web GUI and rebooting. After the reboot your router will connect to the VPN!

1. pfSense ⇒ System ⇒ Cert Manager ⇒ export CA cert (second icon)

2. pfSense ⇒ System ⇒ Cert Manager ⇒ Certificates ⇒ export cert (first icon)

3. pfSense ⇒ System ⇒ Cert Manager ⇒ Certificates ⇒ export key (second icon)

4. Paste certs and key into this script The script is based off hidemyass.com OpenVPN script for DD-WRT. The original is here. Update the variables based on your infrastructure!

5. DD-WRT ⇒ Administration ⇒ Commands ⇒ paste script w/ certs and key ⇒ Save Startup

6. DD-WRT ⇒ Administration ⇒ Management ⇒ Reboot Router

DONE!! Enjoy your VPN!!

Additional Instructions for Redirect Gateway Clients will be unable to access the internet if redirect gateway and automatic outbound NAT are enabled together. Change outbound NAT from automatic to manual. Don’t worry. Automatic rules will fill the table after you activate manual mode. Then add the client’s subnet to the outbound NAT map.

pfSense ⇒ Firewall ⇒ NAT ⇒ Outbound ⇒ select manual ⇒ save

pfSense ⇒ Firewall ⇒ NAT ⇒ Outbound ⇒ add new Source: Type: Network Source: Address: Enter the subnet you want traffic to be redirected for. Example: to redirect Mike’s traffic we would enter 10.1.1.0 here.

Save. Apply.