SITE-TO-SITE VPNS PART IV: VYATTA

A free version of the new Vyatta 6.4 with a remarkable straight-forward configuration for VPN if you're getting familiar with the concepts (which, if you've read the first three parts of this series, should be the case now). Just like the previous example, this will use 3DES, MD5, PFS, DH Group 2, and some default lifetimes. Vyatta also supports SHA and AES-128 and AES-256. Strange but true: AES-192 does not seem to be an option. If anything is unclear,

On to the config. To cover it completely, first the interface configuration and a default route, as the VPN relies on routes to decide where to route traffic before encryption (just like the Cisco devices).

set interfaces ethernet *eth0* address *ip-address/netmask*

set protocols static route 0.0.0.0/0 next-hop *gateway-address*

Phase 1 parameters:

set vpn ipsec ike-group *IKE* lifetime 86400

set vpn ipsec ike-group *IKE* proposal 1 encryption 3des

set vpn ipsec ike-group *IKE* proposal 1 hash md5

set vpn ipsec ike-group *IKE* proposal 1 dh-group 2

Just like with Cisco, the proposal number is for the order in which the different proposals are examined. Phase 2 is no different from that:

set vpn ipsec esp-group *ESP* lifetime 3600

set vpn ipsec esp-group *ESP* mode tunnel

set vpn ipsec esp-group *ESP* proposal 1 encryption 3des

set vpn ipsec esp-group *ESP* proposal 1 hash md5

set vpn ipsec esp-group *ESP* pfs dh-group2

PFS is optional, of course. Now, IPsec has to be activated on a per-interface basis. Again, a simple command for the outgoing interface:

set vpn ipsec ipsec-interfaces interface *eth0*

Finally, the definition of a VPN peer, it's parameters, shared key, local and remote subnets, and Phase 1 and Phase 2 proposals:

set vpn ipsec site-to-site peer *peer-ip-address*

set vpn ipsec site-to-site peer *peer-ip-address* local-ip *local-address*

set vpn ipsec site-to-site peer *peer-ip-address* authentication pre-shared-secret *key*

set vpn ipsec site-to-site peer *peer-ip-address* ike-group *IKE*

set vpn ipsec site-to-site peer *peer-ip-address* tunnel 1 esp-group *ESP*

set vpn ipsec site-to-site peer *peer-ip-address* tunnel 1 local subnet *source-network/mask*

set vpn ipsec site-to-site peer *peer-ip-address* tunnel 1 remote subnet *destination-network/mask*

That's it. In fact, I've found this to be one of the most simply CLI-based VPN configurations I've come across so far. The only thing slightly different from most configurations is the requirement of the local-ip parameter. Usually, this is set to the IP address of the outgoing interface, but it can be interesting to set this to a loopback address for which a route is known, so failure of a physical interface does not terminate the VPN connection.

Source : http://reggle.wordpress.com/2012/11/15/site-to-site-vpns-part-iv-vyatta/