TheGreenBow IPSec VPN klient

Konfigurační příručka k VPN routerům Planet

http://www.thegreenbow.com
http://www.planet.com.tw

Obsah:

1. Úvod

1.1 Účel příručky

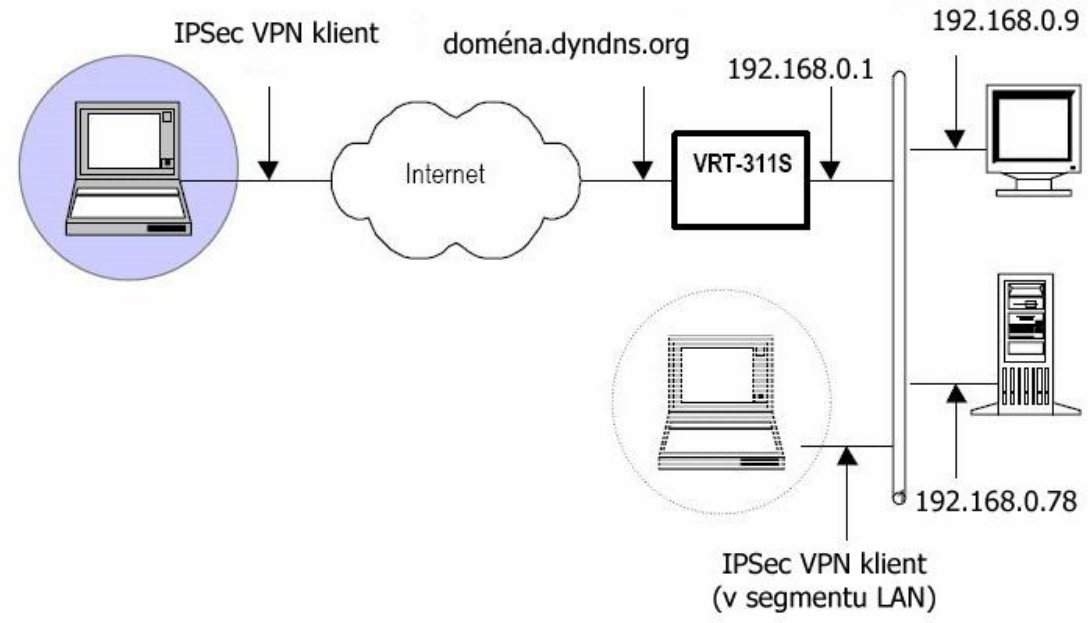
Tato konfigurační příručka popisuje jak nastavit TheGreenBow IPSec VPN klienta s VPN routery od společnosti Planet.

1.2 Topologie VPN sítě

V uvedeném případě VPN sítě (diagram viz. níže) je softwarový IPSec klient připojen k routeru VRT-311S a tunelem do sítě LAN nacházející se za ním. Klient je připojen do internetu přes DSL připojení nebo přes bezdrátové připojení. Veškeré uvedené adresy v této příručce jsou však pouze jako demonstrativní, ve Vašem případě se budou pak zajisté lišit.

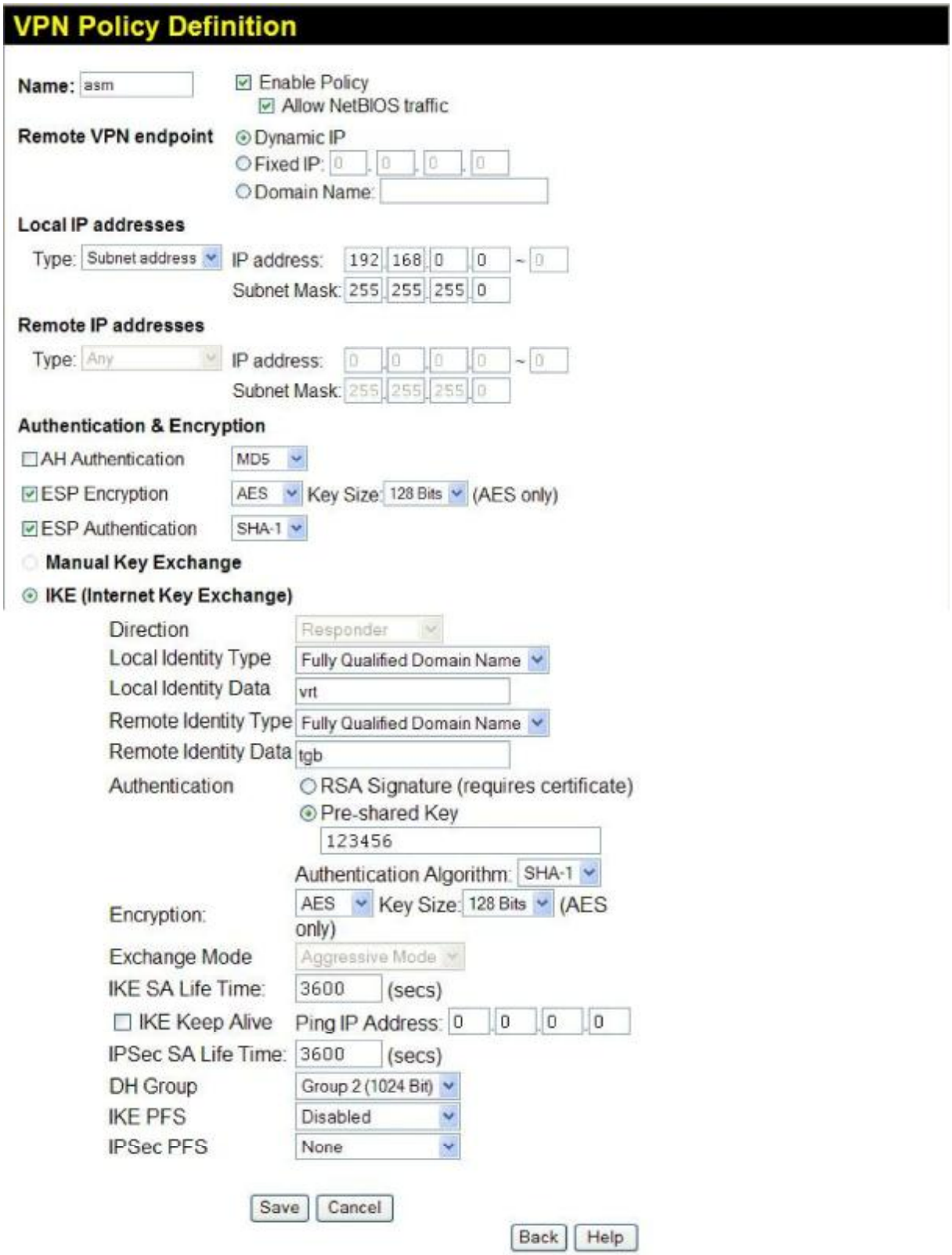
Příklad:

Externí IP adresa VRT311S: doména.dyndns.org (nebo veřejná IP adresa)
IP subnet za VRT311S: 192.168.0.0/255.255.255.0



2 VRT311S VPN konfigurace

V routeru VRT-311S jděte přes menu do „VPN policies“ a nadefinujte nové pravidlo:



AES algoritmus jako metoda šifrování je více efektivní než metody DES a 3DES (je rychlejší pro vlastní propustnost a je více bezpečnější), použít však můžete i jiné z nabídky routeru.

„Aggressive mode“ je zvolena automaticky pro způsob „roadwarrior“ přístup. „PFS“ v tomto režimu nesmí být použito. V příkladu je pro lokální a vzdálenou identitu je zvolen název domén, lze však použít libovolnou identitu.

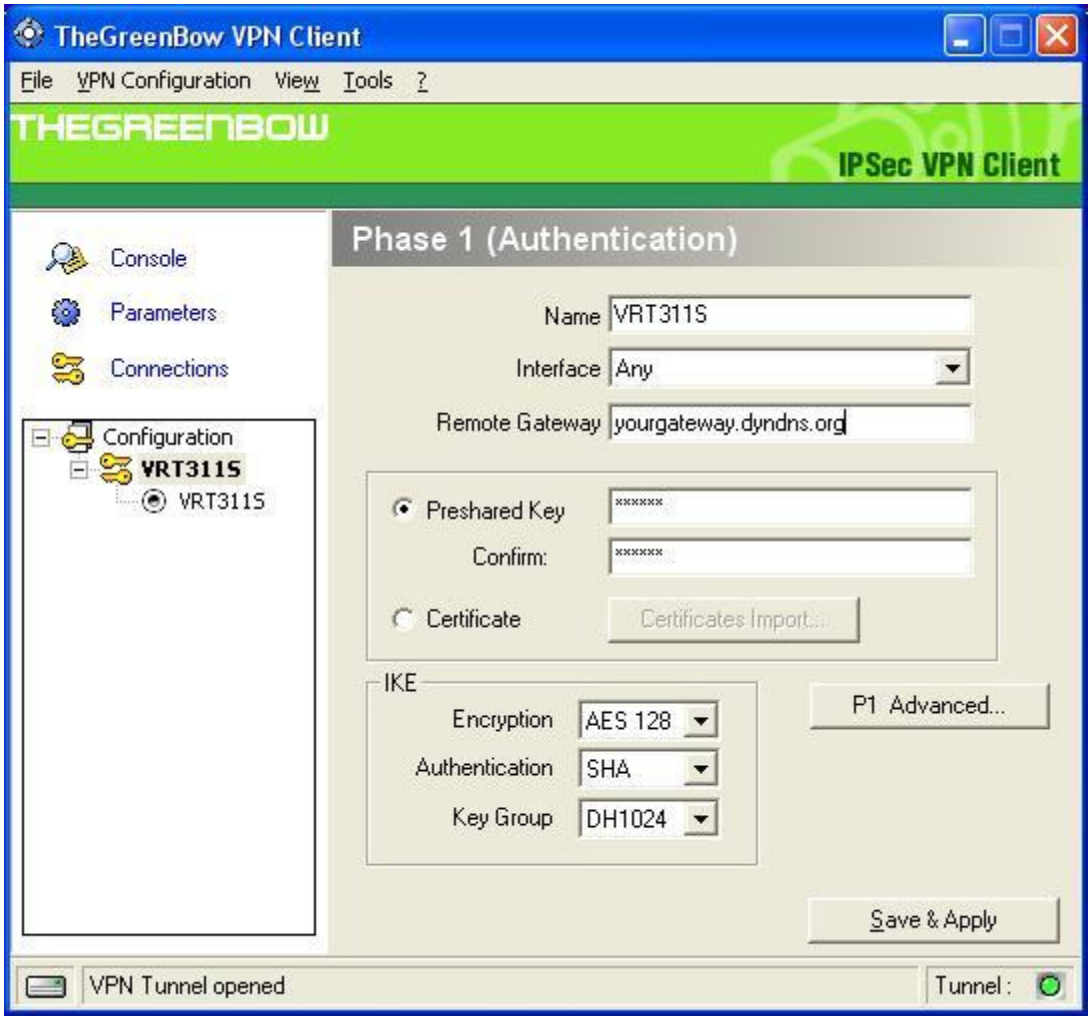
V příkladu je použita metoda pro výměnu šifry přes před-sdílený klíč „preshared key“, lze použít i způsob výměny šifer přes naimportovaný certifikát přidělený od CA-certifikační autority, IDs pak nastavte na „DER_ASN1_DN“.

3 Konfigurace TheGreenBow IPSec VPN klienta

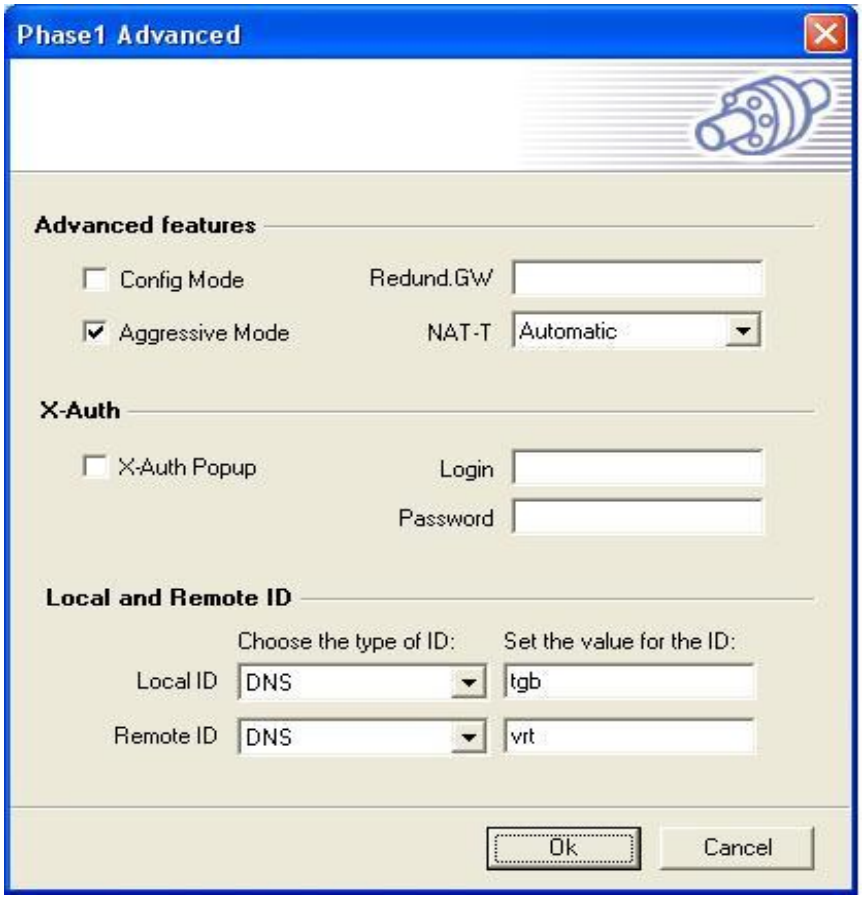
3.1 VPN klient - konfigurace „Phase 1“

Klikněte pravým tl.myši na „Configuration“ v TheGreenbow VPN klientovi a vyberte „Add Phase 1“. Pak vyberte „new phase 1“. Hodnoty které bude třeba změnit a vložit jsou uvedeny níže. Předsdílený klíč uvedený v příkladu je příliš krátký, v provozu používejte delší, zachovejte zásady pro tvorbu hesel.

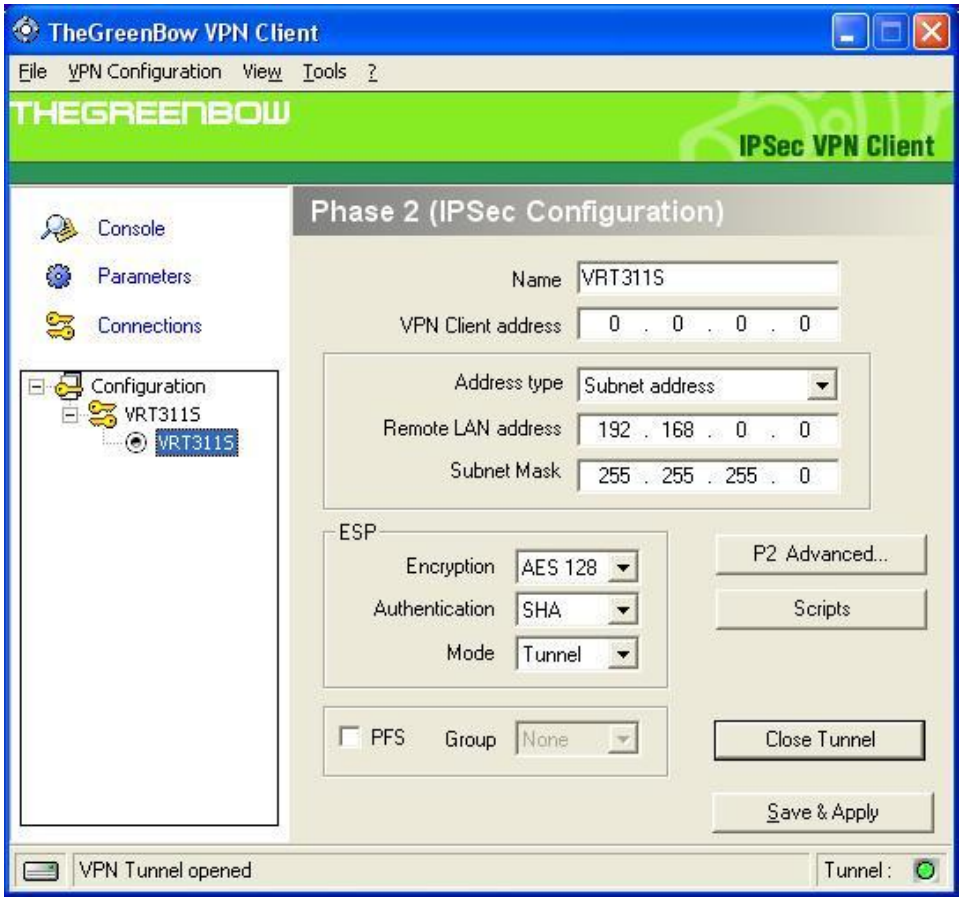
Konfigurace Phase 1



Klikněte na „P1 advanced“ pro zvolení aggressive módu, zvolte a zadejte identifikační parametry.



3.2 Konfigurace VPN klienta „Phase 2“



„0.0.0.0“ ve ”VPN client address” znamená IP adresu pro VPN klienta pro toto konkrétní připojení pro PC síťový adaptér.

„Phase 2 advanced“ slouží pro zadání parametrů pro alternativní DNS nebo WINS servery. Pokud jsou nakonfigurovány, tyto adresy pak přepíší defaultní DNS/WINS parametr serveru v hlavičce IP paketu při provozu IPSec tunelu. Po rozpojení se vrací hodnoty DNS apod. na původní hodnoty nadefinované lokálně na klientském PC.

4 VPN IPSec řešení problémů

4.1 « PAYLOAD MALFORMED »

114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification type PAYLOAD_MALFORMED
114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error

Pokud se setkáte s chybou « PAYLOAD MALFORMED » pravděpodobně jsou špatně nastaveny parametry pro Phase 1 [SA], zkontrolujte si nastavení šifrovacích algoritmů, zda jsou stejné na obou stranách IPSec tunelu.

4.2 « INVALID COOKIE »

115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification type INVALID_COOKIE
115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error

« INVALID COOKIE » chyba znamená, že jedna strana ze zakončení tunelu používá „SA“ které již pozbylo platnosti. Resetujte spojení na jedné ze stran IPSec tunelu.

4.3 « no keystate »

115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50

Zkontrolujte zda předsdílený klíč je nastaven správně a jestli lokální identita „local ID“ je zvolena a vyplněna stejným způsobem jako na druhé straně.

4.4 « received remote ID other than expected »

120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected

Hodnota « Remote ID » (v nastaveních « Advanced ») nekoresponduje s protistranou.

4.5 « NO PROPOSAL CHOSEN » error

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational [HASH][DEL]
115915 Default CNXVPN1-P1 deleted

Při chybě « NO PROPOSAL CHOSEN » zkontrolujte zda « Phase 2 » šifrovací algoritmus je stejný na obou stranách VPN Tunelu.

Zjistěte zda log pro « Phase 1 » vypisuje toto:

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error

4.6 « INVALID ID INFORMATION »

122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode [SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION
122626 Default RECV Informational [HASH][DEL]
122626 Default CNXVPN1-P1 deleted

Pokud se objeví « INVALID ID INFORMATION », zkontrolujte zda « Phase 2 » ID (lokální adresa a síťová adresa) je v pořádku a koresponduje s protější „repote“ stranou. Zkontrolujte také „ID type“ (masku podsítě a adresu pro LAN). Pokud Vám maska není známa, použijte přímo pro „remote LAN“ typ IPV4_ADDR ne tedy „IPV4_SUBNET type“.

4.7 Kliknul jsem na “Open tunnel”, nic se však nestalo.

Přečtěte si logy na každé straně tunelu, IKE požadavky na protistranu mohou být odmítnuty firewally v cestě. IPSec klienti používají port 500 UDP, port 4500 UDP pro protokol ESP (protokol 50).

4.8 VPN tunel již běží, ale není možné získat odpověď na příkaz ping od protistrany.

Pokud VPN tunel běží a přesto si nelze pinknout na vzdálený segment LAN, zkuste:

- Zkontrolujte nastavení pro „Phase 2“: adresu VPN klienta a vzdálené LAN sítě, obvykle není parametr nastaven správně podle vzdáleného rozsahu LAN segmentu.

- Pokud je VPN tunel již sestaven, pakety jsou posílány ESP protokolem. Tento protokol nesmí být blokovaný na firewallech. Zkontrolujte, zda síťová zařízení v cestě ho neblokují, přesměrujte příslušný port.

- Zkontrolujte log VPN serveru, pakety mohou být zahazovány některým z firewall pravidel.

- Zajistěte si u vašeho ISP podporu přenosuprotokolu ESP.

- Zkontrolujte nastavení „výchozí brány“ na VPN serveru pro zařízení v segmentu jeho LAN. Vzdálená zařízení mohou obdržet požadavek ping, nemohou však bez „gateway“ odpovědět.

5 Kontakty

Novinky a updaty na TheGreenBow: http://www.thegreenbow.com
Prodej a podpora: http://www.asm.cz