

TRIỂN KHAI KẾT NỐI VPN IPsec SITE-TO-SITE GIỮA PFSENSE VÀ DRAYTEK

1. Mục tiêu

Thiết lập một đường hầm VPN (Virtual Private Network) an toàn theo phương thức Site-to-Site, cho phép các mạng LAN ở hai địa điểm khác nhau có thể giao tiếp với nhau một cách minh bạch và bảo mật thông qua Internet.

2. Sơ đồ hệ thống và Thông số Cấu hình

Thuộc tính	Site 1 (Văn phòng NVT)	Site 2 (Văn phòng Tân Hường)
Thiết bị	Tường lửa pfSense	Router DrayTek Vigor 2960
IP WAN Public	113.161.80.147	118.69.187.183
Mạng LAN cần kết nối	VLAN 11: 192.168.11.0/24	LAN 1: 192.168.4.0/24

The image shows the DrayTek Vigor 2960 Series web interface. The top navigation bar includes 'Quick Start Wizard', 'Online Status', 'WAN', 'LAN', 'Routing', and 'NAT'. The 'LAN' section is selected, showing a list of LAN interfaces. The 'LAN1' interface is highlighted, showing its IP address as 192.168.11.251. Below the LAN list, the 'Device Information' section displays details for the Vigor2960, including Model, Hardware, Firmware, and Revision.

Profile	Enable	Description	VLAN ID	IPv4 Protocol	IP Address
Lan1	true	Lan1	10	static	192.168.4.1
Lan2	true	Lan2	20	static	192.168.20.1
Lan3	true	Lan3	30	static	192.168.30.1
Lan4	true	Lan4	40	static	192.168.40.1

3. Tóm tắt Cấu hình Chung Giao thức IPsec

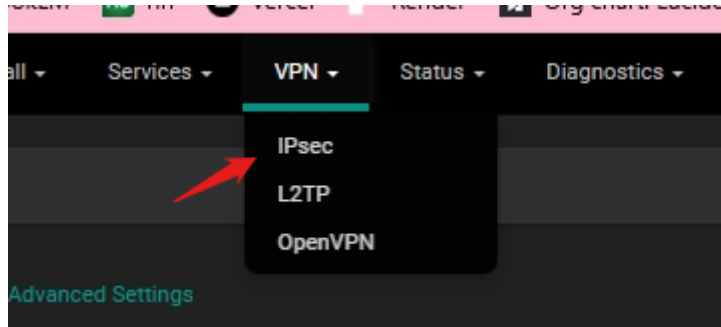
Để kết nối thành công, các tham số mã hóa và xác thực ở cả hai đầu phải được cấu hình đối xứng (giống hệt nhau).

- **Giao thức trao đổi khóa (Key Exchange):** IKEv2
 - **Phương thức xác thực (Authentication):** Khóa chia sẻ trước (Pre-Shared Key - PSK)
 - **Định danh (Identifiers):**
 - pfSense (Site 1): nguyenvanthu.vpn
 - DrayTek (Site 2): tanhuong.vpn
 - **Cấu hình Giai đoạn 1 (Phase 1 Proposal):**
 - **Thuật toán mã hóa (Encryption):** AES 256 bits
 - **Thuật toán băm (Hash):** SHA256
 - **Nhóm Diffie-Hellman (DH Group):** 14 (2048 bit)
 - **Cấu hình Giai đoạn 2 (Phase 2 Proposal):**
 - **Giao thức (Protocol):** ESP (Encapsulating Security Payload)
 - **Thuật toán mã hóa (Encryption):** AES 256 bits
 - **Thuật toán băm (Hash):** SHA256
 - **PFS key group:** 14 (2048 bit)
-

4. Thao tác cấu hình Chi tiết

1. Tạo Tunnel - Giai đoạn 1 (Phase 1):

- Truy cập VPN > IPsec > Tunnels và nhấn Add P1.



- **IKE Endpoint Configuration:**
 - Key Exchange version: IKEv2
 - Interface: WAN (113.161.80.147)
 - Remote Gateway: 118.69.187.183 (IP WAN của DrayTek)

IKE Endpoint Configuration	
Key Exchange version	<input type="text" value="IKEv2"/> <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	<input type="text" value="IPv4"/> <small>Select the Internet Protocol family.</small>
Interface	<input type="text" value="WAN"/> <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	<input type="text" value="118.69.187.183"/> <small>Enter the public IP address or host name of the remote gateway.</small>

- **Phase 1 Proposal (Authentication):**
 - Authentication Method: Mutual PSK
 - My identifier: Fully qualified domain name - nguyenvanthu.vpn
 - Peer identifier: Fully qualified domain name - tanhuong.vpn
 - Pre-Shared Key: Nhập khóa bí mật đã thống nhất.

Phase 1 Proposal (Authentication)	
Authentication Method	<input type="text" value="Mutual PSK"/> <small>Must match the setting chosen on the remote side.</small>
My identifier	<input type="text" value="Fully qualified domain name"/> <input type="text" value="nguyenvanthu.vpn"/>
Peer identifier	<input type="text" value="Fully qualified domain name"/> <input type="text" value="tanhuong.vpn"/>
Pre-Shared Key	<input type="text" value="Novaon@2025"/> <small>Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.</small> Generate new Pre-Shared Key

- **Phase 1 Proposal (Encryption Algorithm):**
 - Cấu hình các thuật toán mã hóa và băm như đã nêu ở mục 3.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm	Algorithm	Key length	Hash	DH Group	
AES	Algorithm	256 bits	SHA256	14 (2048 bit)	Delete

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm [+ Add Algorithm](#)

2. Tạo Tunnel - Giai đoạn 2 (Phase 2):

- Trong tunnel Phase 1 vừa tạo, nhấn Show Phase 2 Entries và Add P2.

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol
	1	V2	WAN 118.69.187.183	Mutual PSK	AES (256 bits)

[Show Phase 2 Entries \(1\)](#)

- **Networks:**
 - Local Network: Chọn VLAN11 subnet (tức là 192.168.11.0/24). Đây là mạng LAN nội bộ cần chia sẻ qua VPN.
 - Remote Network: Nhập 192.168.4.0/24. Đây là mạng LAN từ xa của văn phòng Tân Hương.

Phase 2 Proposal (SA/Key Exchange)

Local Network	NAT/BINAT translation	Remote Network
VLAN11 subnet	None	Network
Type	Type	Type
Local network component of this IPsec security association.	If NAT/BINAT is required on this network specify the address to be translated	Remote network component of this IPsec security association.
Address	Address	Address

- **Phase 2 Proposal (SA/Key Exchange):**
 - Cấu hình các thuật toán mã hóa và băm tương ứng với Giai đoạn 1.

Phase 2 Proposal (SA/Key Exchange)

Protocol ESP
 Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms ☒ AES 256 bits

☐ AES128-GCM Auto

☐ AES192-GCM Auto

☐ AES256-GCM Auto

☐ CHACHA20-POLY1305

Hash Algorithms ☐ SHA1 ☒ SHA256 ☐ SHA384 ☐ SHA512 ☐ AES-XCBC
 Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group 14 (2048 bit)
 Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

3. Cấu hình Quy tắc Tường lửa (Firewall Rules):








- Truy cập Firewall > Rules > IPsec.
- Tạo một quy tắc mới cho phép lưu lượng (traffic) từ bất kỳ nguồn nào (any) đến bất kỳ đích nào (any) đi qua giao diện IPsec. Điều này cho phép các mạng LAN giao tiếp với nhau qua đường hầm VPN vừa tạo.








Firewall / Rules / IPsec

Floating WAN LAN VLAN11 VLAN12 VLAN13 VLAN14 VLAN15 VLAN16 WAN1 WAN2 WAN3 **IPsec**

OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/158 KIB	IPv4 *	*	*	*	*	none			      

Site Tân Hương (DrayTek)

1. Tạo Hồ sơ VPN (VPN Profile):

- Truy cập VPN and Remote Access > VPN Profiles, nhấn Add để tạo một hồ sơ mới.
- **Dial-Out Settings:**
 - Dial-Out Through: Chọn cổng WAN1.
 - Remote Host: 113.161.80.147 (IP WAN của pfSense).
 - Local IP / Subnet Mask: 192.168.4.0/24 (Mạng LAN nội bộ).
 - Remote IP / Subnet Mask: 192.168.11.0/24 (Mạng LAN từ xa của pfSense).

The screenshot shows the 'Dial-Out Settings' section of the pfSense VPN Profiles configuration. The 'Auto Dial-Out' option is set to 'Enable' with a dropdown menu set to 'Always Dial-Out'. The 'For Remote Dial-In User' option is set to 'Disable'. The 'Dial-Out Through' dropdown is set to 'wan1', and the 'Default WAN IP' radio button is selected. The 'Failover to' dropdown is empty. The 'Local IP / Subnet Mask' is set to '192.168.4.0' with a subnet mask of '255.255.255.0/24'. The 'Local Next Hop' is set to '0.0.0.0' with a note '(0.0.0.0 : default gateway)'. The 'Remote Host' is set to '113.161.80.147'. The 'Remote IP / Subnet Mask' is set to '192.168.11.0' with a subnet mask of '255.255.255.0/24'.

2. Cấu hình IKE và Mã hóa:

- **IKE Protocol:** Chọn IKEv2.
- **Auth Type:** Chọn PSK và nhập đúng Pre-Shared Key đã cấu hình trên pfSense.
- **Local ID / Remote ID:** Nhập tanhuong.vpn và nguyenvanthu.vpn tương ứng.

The screenshot shows the 'IKE and Encryption' section of the pfSense configuration. The 'IKE Protocol' is set to 'IKEv2'. The 'Auth Type' is set to 'PSK'. The 'Preshared Key' field contains a series of asterisks. The 'Local ID' is set to 'tanhuong.vpn' with a note '(optional)'. The 'Remote ID' is set to 'nguyenvanthu.vpn' with a note '(optional)'. The 'Security Protocol' is set to 'ESP'.

3. Chuyển sang tab **Advanced > Proposal**.
4. **IKE Phase1/Phase2 Proposal:** Chọn các thuật toán mã hóa (AES256), xác thực (SHA2_256), và nhóm DH (G14) để khớp chính xác với cấu hình trên pfSense.

The screenshot shows the pfSense configuration page for a VPN profile named 'vpn_th_nvt'. The 'Enable' checkbox is checked. The 'Proposal' tab is selected among 'Basic', 'Advanced', 'GRE', 'Proposal', and 'Multiple SAs'. The configuration for the proposal is as follows:

Field	Value
IKE Phase1 Proposal [Dial-Out] :	AES256 G14
IKE Phase1 Authentication [Dial-Out] :	SHA2_256
IKE Phase2 Proposal [Dial-Out] :	AES256 with auth
IKE Phase2 Authentication [Dial-Out] :	SHA2_256
Accepted Proposal [Dial-In] :	acceptall

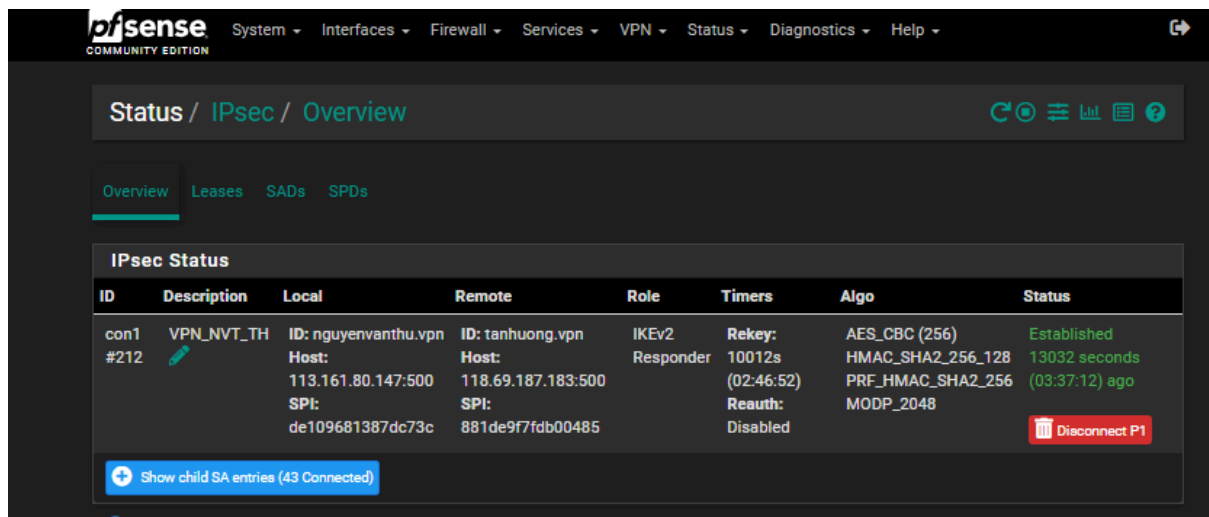
5. **Lưu và Kích hoạt:**

- Lưu lại toàn bộ cấu hình. Hồ sơ VPN sẽ được kích hoạt và tự động quay số kết nối đến pfSense.
-

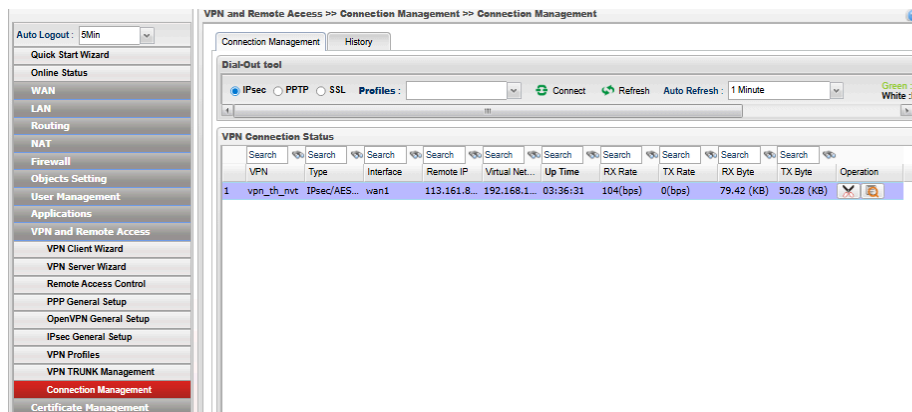
5. Kiểm tra và Xác thực Kết nối

Sau khi hoàn tất cấu hình ở cả hai phía, trạng thái kết nối đã được kiểm tra và xác nhận thành công:

- **Trên pfSense:** Tại Status > IPsec, tunnel hiển thị trạng thái **"Established"**, cho thấy Giai đoạn 1 và Giai đoạn 2 đã được thiết lập thành công.



- **Trên DrayTek:** Tại VPN and Remote Access > Connection Management, tunnel hiển thị trạng thái kết nối, thời gian uptime, và có lưu lượng dữ liệu (RX/TX bytes) đang được truyền qua.



Quá trình cấu hình kết nối VPN IPsec Site-to-Site giữa tường lửa pfSense và router DrayTek Vigor 2960 đã hoàn tất thành công. Đường hầm VPN đã được thiết lập ổn định, đảm bảo luồng giao tiếp an toàn và thông suốt giữa hai mạng LAN 192.168.11.0/24 và 192.168.4.0/24. Hệ thống đã sẵn sàng cho việc trao đổi dữ liệu nội bộ giữa hai văn phòng.

