

DrayTek



Agenda

DrayOS4 Router:

Vigor2927L-5G series

Vigor3912(S)

DrayOS 5 Router:

Vigor1100_v2 series

Vigor2136 series

DrayOS 5 AP:

AP1062C

AP962C

New Products

- Router
- **Vigor2927L-5G series**
- Vigor3912(S)



Vigor2927L-5G Series Router



5G 2800/555 Mbps

5G Band 1/3/7/8/20/28/40/77/78

LTE 4G backward compatible

Cat. 19 1600/200 Mbps

1x GbE WAN

1x GbE Switchable WAN/LAN

5x GbE LAN

1x USB 2.0

Wireless

2x2, 2.4GHz, 802.11b/g/n/ax, 574 Mbps

2x2, 5GHz, 802.11 a/n/ac/ax, 2402 Mbps

Vigor2927L-5G Series Router



① Fixed WAN Port	1 x GbE RJ-45
② Switchable WAN/LAN Port	1 x GbE RJ-45
③ Fixed LAN Port	5 x GbE RJ-45
④ USB Port	1 x USB2.0

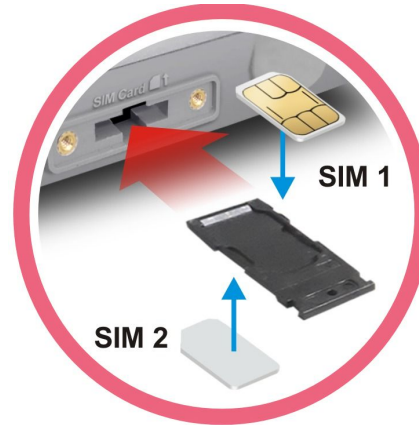
Vigor2927L-5G Series Router



① 2 x WLAN Antennas

② 4 x LTE Antennas

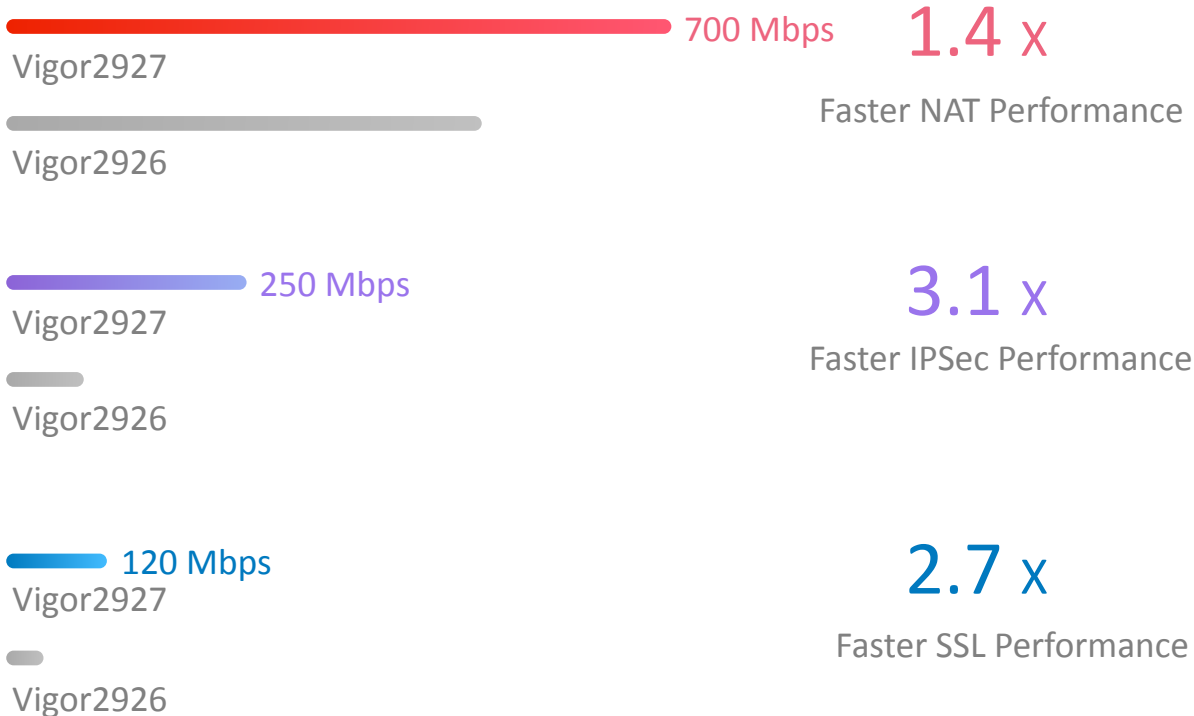
③ Dual SIM Slot



5G Embedded Dual-WAN VPN Firewall Router

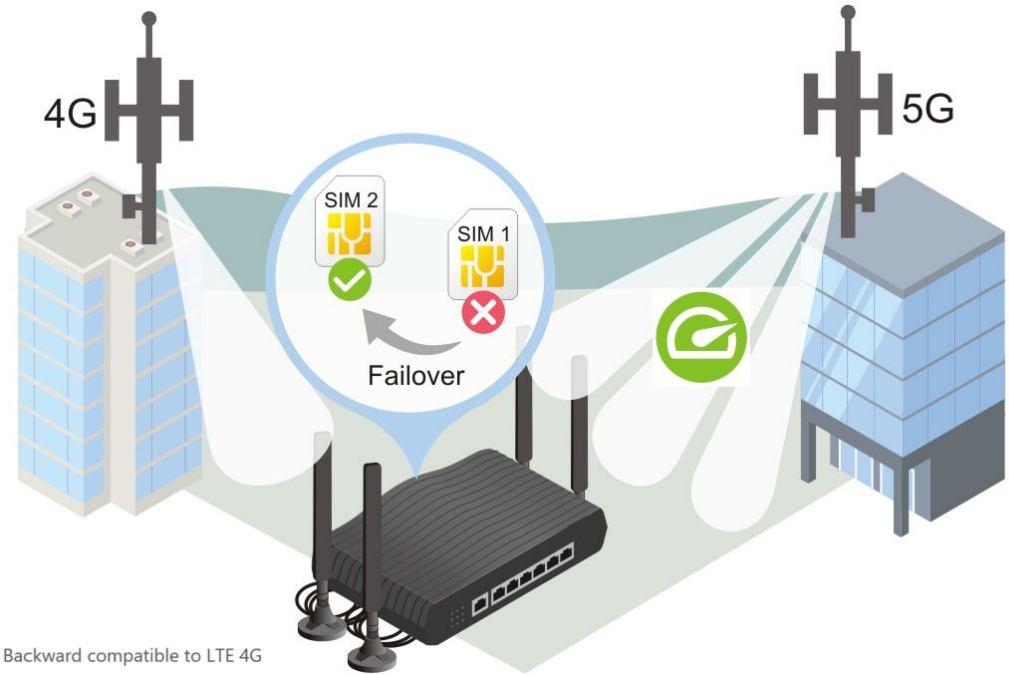
5G & WiFi6 for Next-Gen Connectivity

Vigor2927L-5G Series is a Dual-WAN VPN Router with embedded 5G cellular connectivity. Two SIM slots (1 SIM online at a time) are prepared to deliver an uninterrupted cellular network connection. Featuring VPN, QoS, route policy, web content filtering, hotspot web portal, and more. It is ideal for companies that require higher-performance 5G connectivity with an efficient network. The series includes built-in 802.11ax models.



5G Router with High Speed Mobile Connectivity

- Integrated 5G/LTE modem with Category 19, the carrier aggregation method can get high-speed mobile broadband connectivity for Internet access and VPN.
- Dual-SIM Slot allows using two mobile network providers. So that in the event of one mobile network not providing Internet connectivity, the router can switch to a secondary SIM and cellular network connection.
- Four LTE antennas with 1M extension cables allow users to find the optimum position to install the router to get the best signal reception.



Dual Gigabit + 5G WAN Load Balancer

WAN Load Balancing

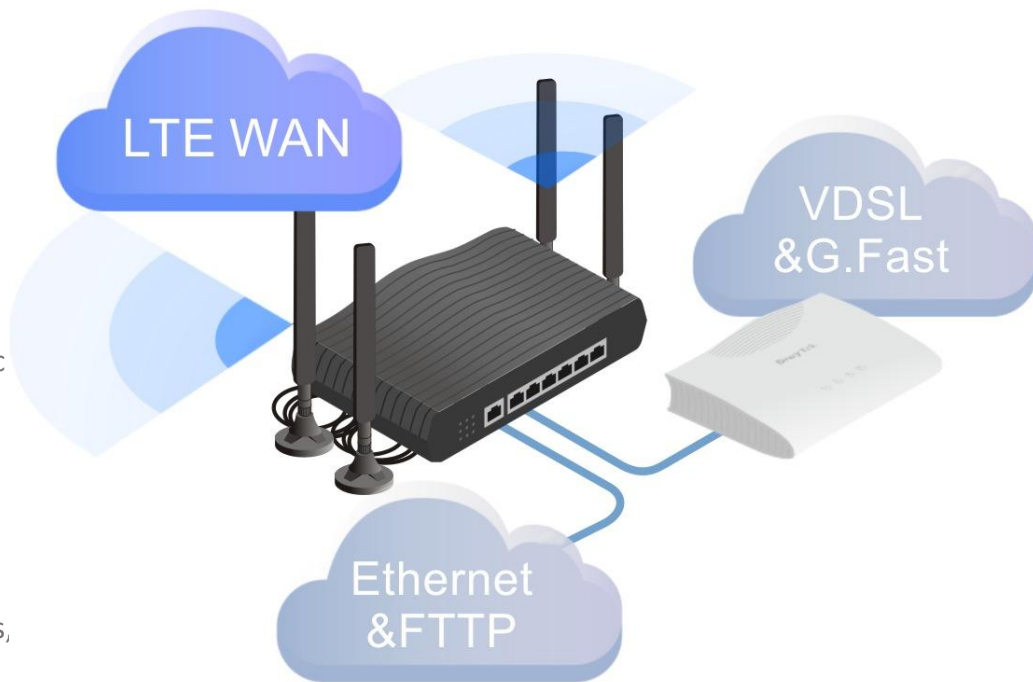
Vigor2927L-5G offers high throughput with load-balancing connectivity, suitable for handling fiber to the premises (FTTP) and gigabit Internet connections. The 5G LTE WAN can provide high-speed mobile broadband connectivity. All the active WANs will automatically join the WAN Load Balance Pool to optimize Bandwidth Utilization.

Seamless Failover

Can do automatic failovers between WAN connections. In the events of ISP outage, the router will transfer the traffic to another WAN smoothly. Ensure reliable Internet connectivity and save you from the cost of network downtime.

Policy-Based Routing

Using routing policies to designate a WAN interface for Applications, VoIP traffic, traffic from a certain range of IPs, or traffic to a specific destination enhances network efficiency and fluency.



Ideal VPN Router for SMB

Fast IPsec Performance

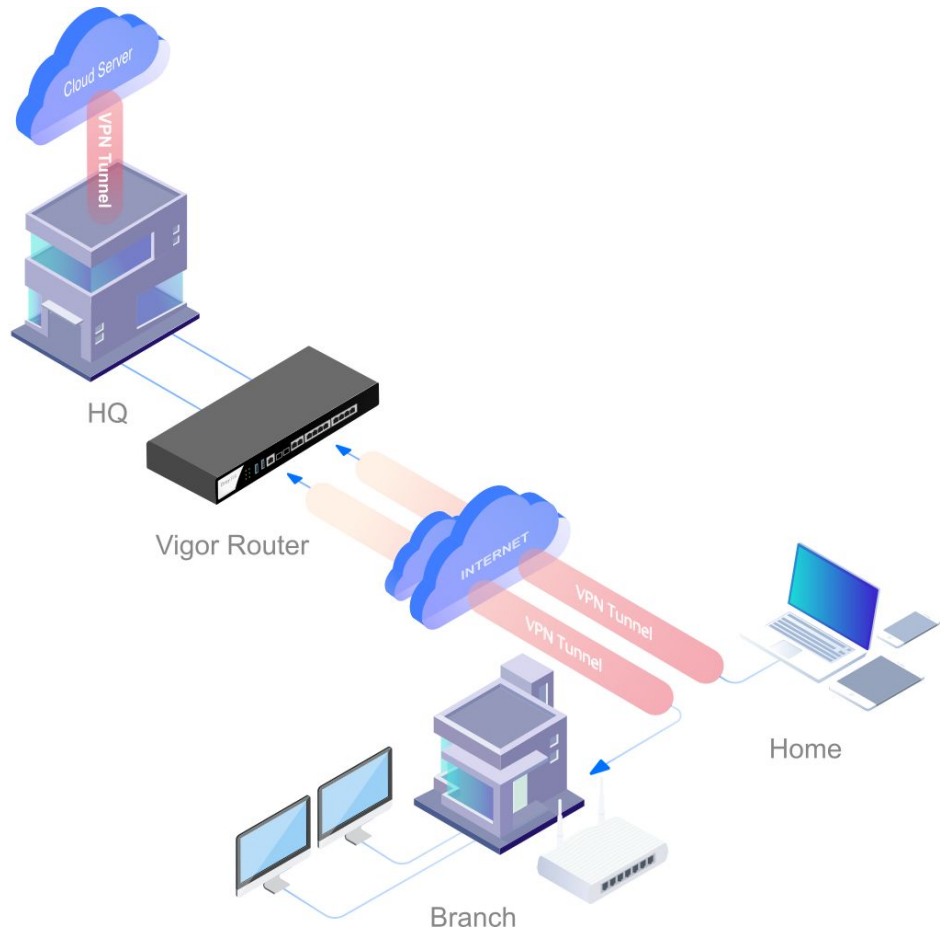
- Hardware Accelerated IPsec VPN Performance
~ 800Mbps
- Up to 50 concurrently active VPN tunnels.

All common VPN standards are supported

- WireGuard is added since fw 4.4.3.
- IKEv1 / IKEv2 EAP / SSL VPN / L2TP over IPsec / PPTP / OpenVPN are all supported.

Advanced Authentication for Teleworker

- 2-factor authentication available for Teleworker VPN connections.
- Authentication can be done with the Active Directory (LDAP) or RADIUS or TACACS+ server in the network.
- Notify User by SMS/Email notification when a Teleworker VPN is online to prevent VPN credential lost and misused by the others.



Market Business with Hotspot Web Portal

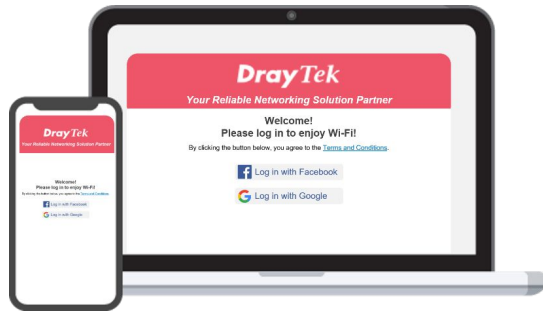
Market your business when providing free Wi-Fi.

Wi-Fi Marketing

Redirect the hotspot guests to the company homepage, online surveys, or display promotion message.

Grow Your Email List

Require the guest to leave contact info or social media accounts before they can use the Internet service.



Various Authentication Type

A variety of login methods are supported to meet your business need, including Facebook Login, Google Login, SMS PIN, Voucher PIN, and RADIUS.

3rd-Party Service Compliant

Supports external captive portal authentication. You can keep using the Wi-Fi marketing solution you like.

Quota Management

Bandwidth management is integrated into Hotspot to control the bandwidth and session usage of the Hotspot guests.

Comprehensive Firewall

Object-based Firewall

Group IPs and Services by Object before applying to Firewall rules. Easy to organize the network activities.

Manage Traffics not only from LAN to WAN

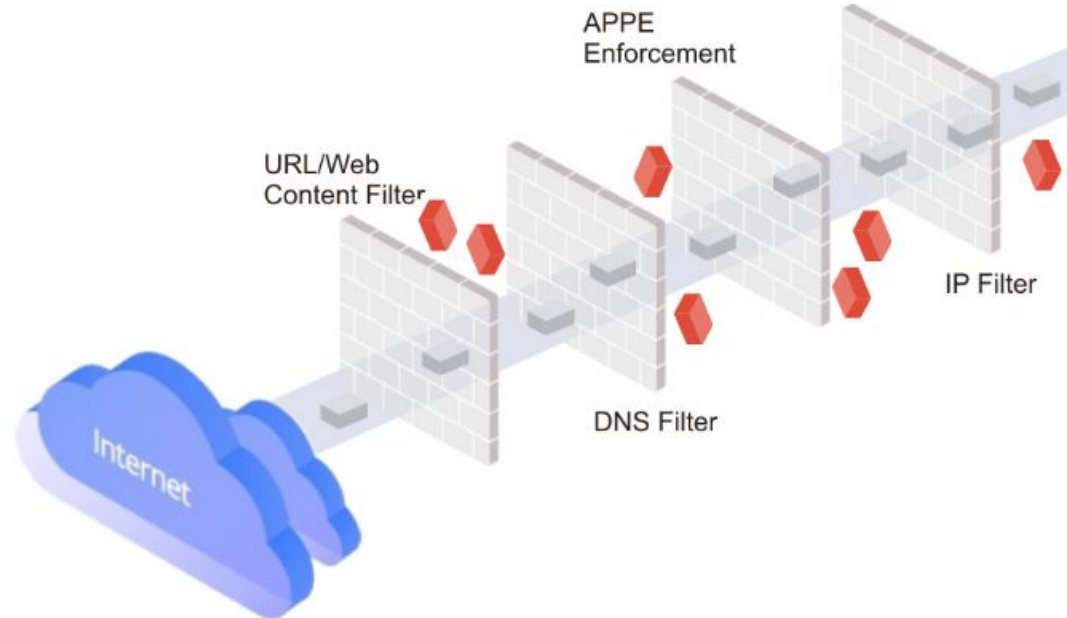
DrayTek's Firewall can manage traffic between LAN subnets, remote VPN subnets, and the traffic from WAN to the Vigor Router itself! Pre-defining the Internet IPs that can access Vigor Router's service is possible.

Web Content Filtering with DNS Filter

Web Content Filtering Service uses cloud-based technology, 82 categories in total, 10 of which are security-focused, providing comprehensive and up-to-date protection to protection to LAN client for their online activities.

Blocking Apps & DoH servers

APP Enforcement (APPE) can easily block applications (IM/P2P/Stream/Tunneling, etc.) on a LAN network with a few clicks. Blocking DoH servers in the browsers can force the LAN clients to use the standard DNS query to make the DNS Filtering work.



APP QoS Bandwidth Management

VoIP First

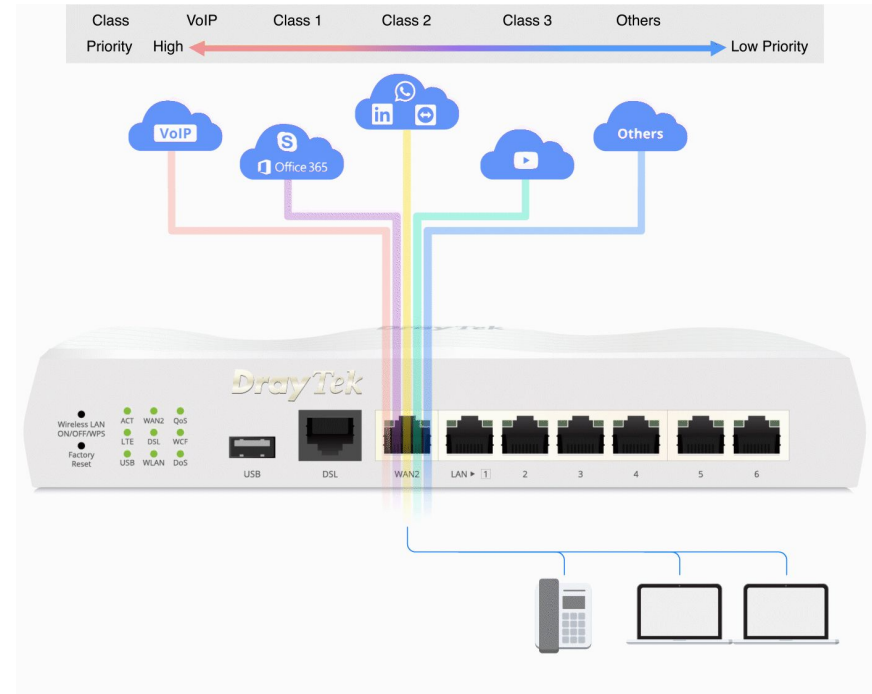
VoIP is always with top priority!
With default UDP 5060 port (configurable), VoIP QoS is out-of-box ready.

Improve Experience for Business-Critical Apps

Select your business critical apps, and easily put them into QoS classes.

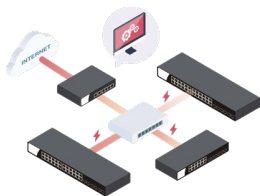
Flexible Bandwidth Allocation

Bandwidth will be reserved for high-priority classes.
With Hardware QoS (Hardware Acceleration Enabled), more bandwidth should be allocated for the high-priority class to guarantee the service runs smoothly.



Designed for Central Management

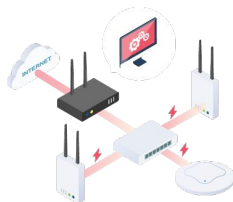
LAN Management



Manage VigorSwitch

10 VigorSwitch

- Automatic Discovery
- Provisioning
- Monitoring
- Centralized Hierarchy View
- Reboot PoE Devices Remotely
- Quick VLAN Configuration

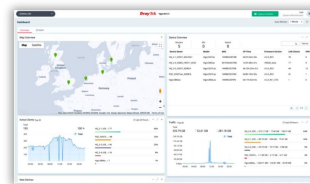


Manage VigorAP

20 VigorAP

- Automatic Discovery
- Automatic Provisioning
- Monitoring
- Centralized View
- Reboot VigorAP Remotely
- Wi-Fi Client Load Balancing

Cloud Managed




Via VigorACS3

(Since ACS V3.6.0 & FW 4.4.5)










- Zero Touch Deployment & Provisioning
- Auto-VPN
- Interface Quality & SLA
- VoIP Optimization & Monitoring
- Application Visibility
- Application-Based SD-WAN Policy
- Customized Hotspot Page with Multilingual
- Hotspot Clients Analytics
- ACS Server Load Balancing / Failover

DrayTek LTE Router Evolution

	Vigor2927L-5G Series	Vigor2927 LTE Series	Vigor2926 LTE Series
			
Fixed WAN Port	1 x GbE RJ-45	1 x GbE RJ-45	1 x GbE RJ-45
Fixed LAN Port	5 x GbE RJ-45	5 x GbE RJ-45	4 x GbE RJ-45
Switchable WAN/LAN Port	1 x GbE RJ-45	1 x GbE RJ-45	1 x GbE RJ-45
USB Port	1 x USB2.0	1 x USB2.0	1 x USB2.0
SIM Slot	2 x Nano-Sized	2 x Standard-Sized	2 x Standard-Sized
4G/5G	4G/5G 	4G	4G
LTE Category	CAT.19 	CAT.6	CAT.4
LTE Max. Rx Link Rate	1600 Mbps 	300 Mbps	150 Mbps
LTE Max. Tx Link Rate	200 Mbps 	50 Mbps	50 Mbps
Max. Number of NAT Sessions	60k	60k	50k
Max. concurrent VPN Tunnels	50	50	50

DrayTek LTE Router Evolution

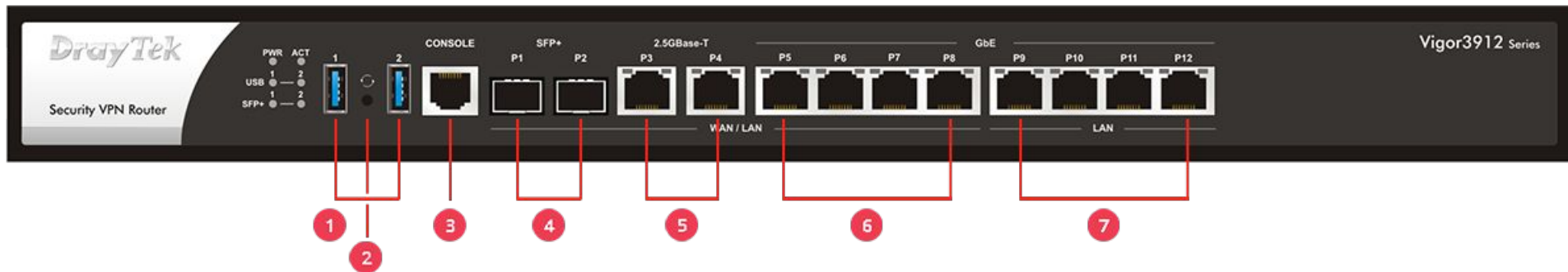
	Vigor2927L-5G Series	Vigor2927 LTE Series	Vigor2926 LTE Series
			
Dual-band Antenna (n/ac/ax model)	2 for ax model 	2 for ac model	2 for n model; 4 for ac model
2.4G WLAN (n/ac/ax model)	802.11 b/g/n/ax 	802.11 b/g/n	802.11 b/g/n
2.4G WLAN Max. Link Rate	574 Mbps 	400 Mbps	300 Mbps
5G WLAN (ac/ax model)	802.11 a/n/ac Wave 2/ax 	802.11 a/n/ac Wave 2	802.11 a/n/ac Wave2
5G WLAN Max. Link Rate	2402 Mbps (2x2)	867 Mbps (2x2)	1.7 Gbps (4x4)
DrayDDNS	✓	✓	✓
Bandwidth Management	✓	✓	✓
Content Filtering	✓	✓	✓
Hotspot Web Portal	✓	✓	✓
Managed via VigorACS	Since ACS 3.6.0; FW 4.4.5	Since ACS 2.5.5; FW 4.2.0	Since ACS 2.3.0; FW 3.8.9
SD-WAN Supported	Since ACS 3.6.0; FW 4.4.5	Since ACS 3.0.0; FW 4.2.0	×

New Products

- Router
- Vigor2927L-5G series
- **Vigor3912(S)**



Vigor3912



1 2x USB 3.0

2 1x Factory Reset Button

3 1x Console RJ45 Port

4 2x 10G/2.5G/1G SFP+ Port*

5 2x 2.5G/1G/100M/10M 2.5GBase-T RJ45 Port*

6 4x 1G/100M/10M Base-T RJ45 Port*

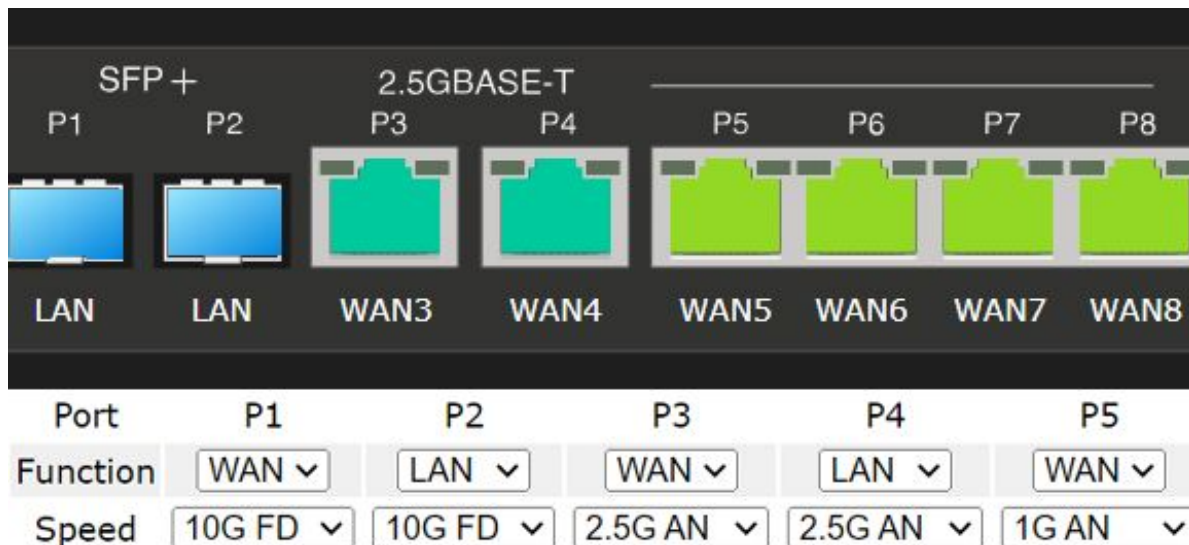
7 4x 1G/100M/10M Base-T RJ45 Port

*WAN / LAN Switchable

Flexible WAN & LAN Ports

12 Ports in total; 8 Ports can be switched to LAN or WAN. So it can have up to

- 8 WAN interfaces with 4 LAN ports; Or
- 1 WAN interface with 11 LAN ports



High Performance 10G Router

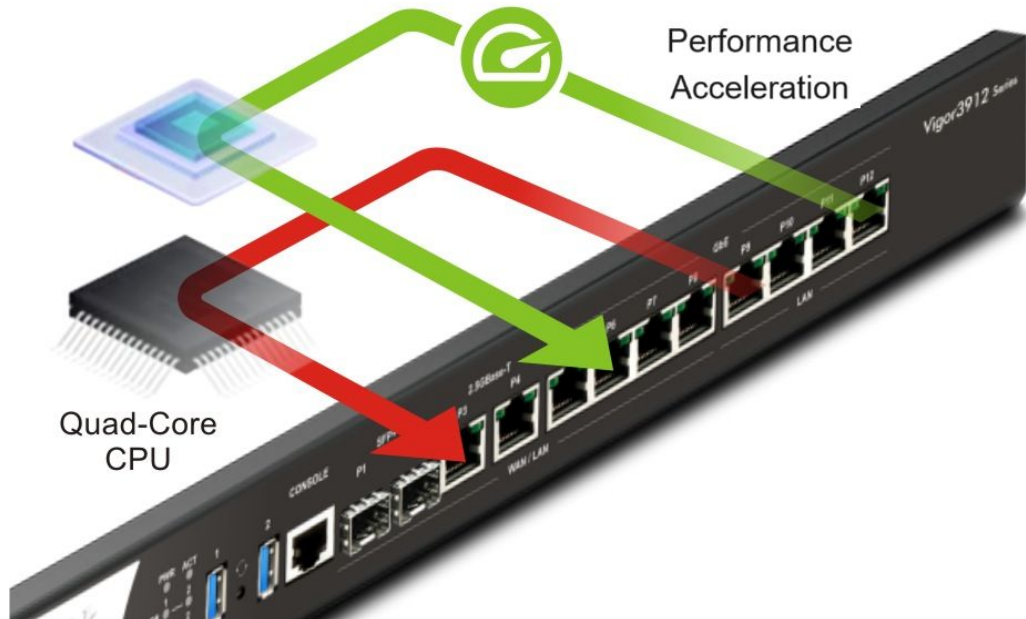
Quad-Core CPU

Provides 15.6 Gbps NAT throughput (bi-directional)

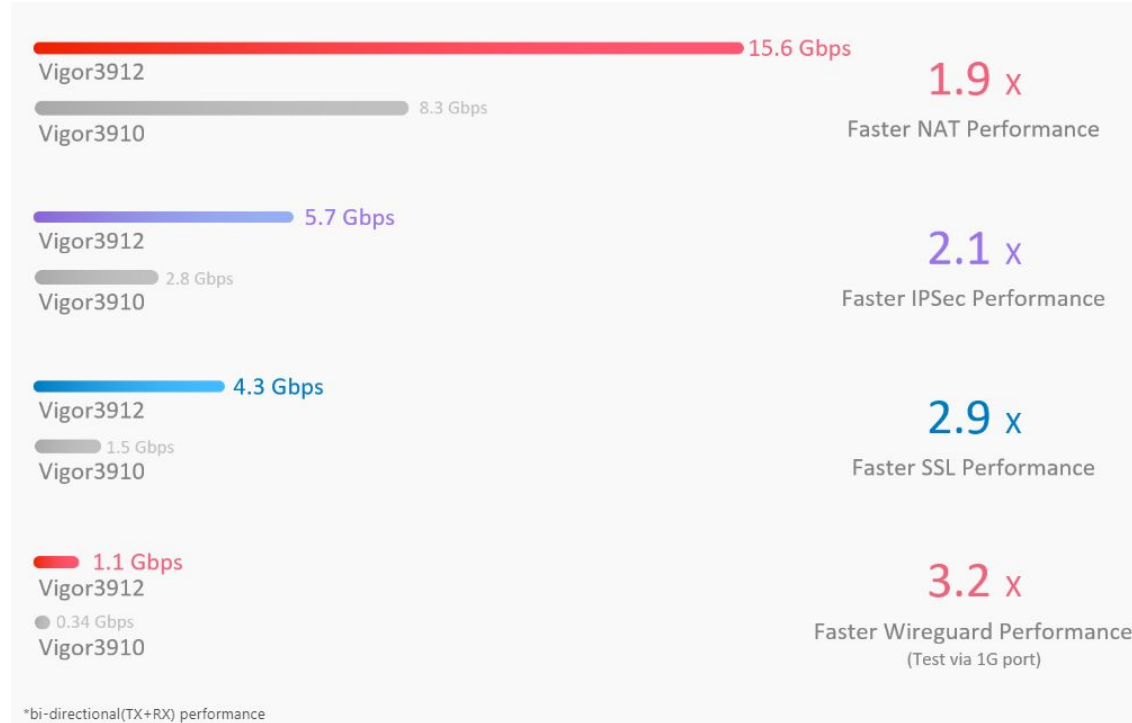
Fast NAT Performance 15.6 Gbps

Fast IPsec Performance 5.7 Gbps

Fast SSL VPN Performance 4.3 Gbps



3912 vs 3910



- approx. **2X** faster than 3910 (for bidirectional traffics)

High Performance VPN Gateway Comparison

	Vigor3912S	Vigor3912	Vigor3910
			
WAN/LAN Port	<u>8 Switchable WAN/LAN</u> 2 x 10 Gigabit SFP+ + 2 x 2.5 GbE RJ-45 + 4 x GbE RJ-45 <u>4 Fixed LAN</u> 4 x GbE RJ-45	<u>8 Switchable WAN/LAN</u> 2 x 10 Gigabit SFP+ + 2 x 2.5 GbE RJ-45 + 4 x GbE RJ-45 <u>4 Fixed LAN</u> 4 x GbE RJ-45	<u>8 Switchable WAN/LAN</u> 2 x 10 Gigabit SFP+ 2 x 2.5 GbE RJ-45 4 x GbE RJ-45 <u>4 Fixed LAN</u> 4 x GbE RJ-45
USB Port	2 x USB 3.0	2 x USB 3.0	2 x USB 3.0
Console Port	1 x RJ-45	1 x RJ-45	1 x RJ-45
Memory	8GB DDR4+256GB SSD	8GB DDR4	2GB DDR4
NAT Throughput	12.5 Gbps (Hardware acceleration is built-in)	12.5 Gbps (Hardware acceleration is built-in)	9 Gbps (Hardware acceleration is built-in)
IPsec VPN Performance	3 Gbps (AES 256 bits)	3 Gbps (AES 256 bits)	2.5Gbps (AES 256 bits)
Max. Number of NAT Sessions	1000K	1000k	500k
Max. concurrent VPN Tunnels	500	500	500
Max. Concurrent SSL VPN	200	200	200
VPN Trunk and Backup	✓	✓	✓
WAN Backup/Failover	✓	✓	✓

New VPN Features

VPN User Isolation

Isolating remote dial-in accounts to protect VPN users from each others. They can only access company's servers but not allowed to enter each other's devices. This helps prevent unauthorized access to sensitive data and protect network from malware or other intrusions.

VPN from LAN (Zero Trust)

Never trust, always verify. VPN from LAN works Zero Trust out. It provides a better security level to your network, which protects vital servers from potential threats caused by other LAN devices. The servers can only be accessed by VPN, even if the devices are on the LAN network.

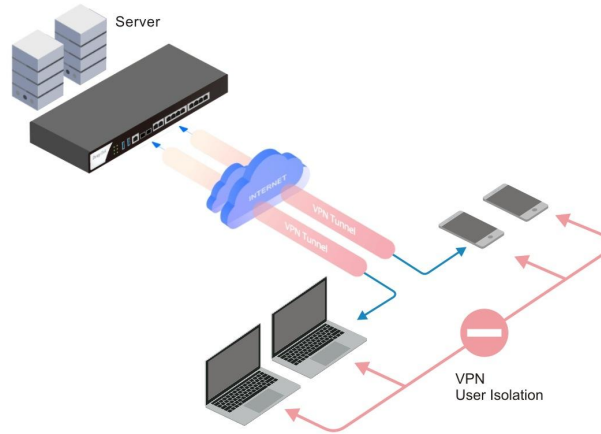
VPN 2FA on AD/LDAP Server

With new Two-Factor authentication, you can strengthen the security of VPN connections and eliminates the expense of SMS messages or license fees in a cost-effective way.

Packet Capture Tool for VPN tunnel

By either mirroring all packets to designated LAN port and now to VPN connection no matter LAN to LAN profile or remote Dial-in users, and even downloading .pcap file via WUI remotely, spotting an issue is easier than ever.

VPN User Isolation



Isolate the VPN users by simply enabling the option "Isolate VPN Users from each other."

<input type="checkbox"/> Enable VPN Remote Dial In from LAN	Selected LAN	?
<input checked="" type="checkbox"/> Isolate VPN Users from each other		

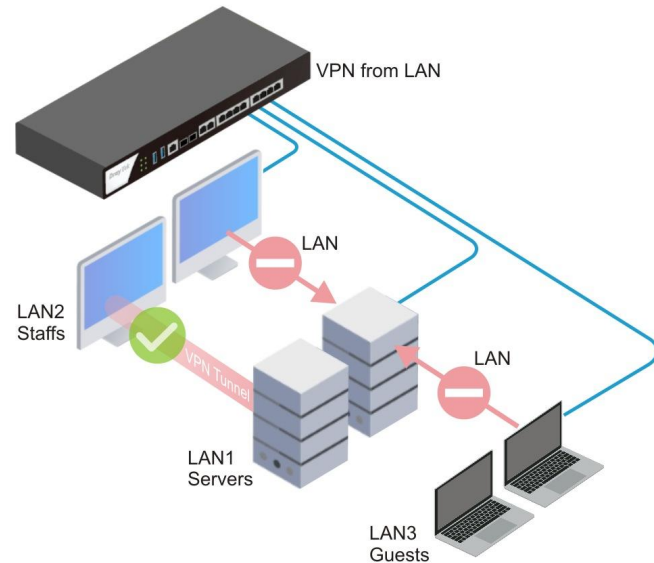
Reference:

<https://www.draytek.com/support/knowledge-base/11437>

VPN From LAN

New 10G High-Performance Load-Balancing VPN concentrator, supports a new VPN from LAN function to increase the security level of your network

For the device or computer that doesn't have a VPN account, it cannot reach the LAN servers.




Reference:

<https://www.draytek.com/support/knowledge-base/11438>

VPN From LAN

1. You can enable VPN Remote Dial-in from a specific LAN

- Go to LAN >> VLAN and LAN General Setup page to create another LAN.
- Select the LAN to allow VPN Dial-In via VPN and Remote Access >> Remote Dial-in User, then Click OK.

LAN >> VLAN 

VLAN Configuration


Enable

	LAN Port						VLAN Tag			
	P2	P4	P9	P10	P11	P12	Subnet	Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input type="checkbox"/>	0	0
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 3	<input type="checkbox"/>	0	0

LAN >> General Setup

General Setup

Index	Description	Enable	DHCP	IP Address
LAN 1	Server	V	V	172.17.5.3
LAN 2	Staff	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10.3.0.3
LAN 3	Guests	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1
IP Routed Subnet		<input type="checkbox"/>	<input type="checkbox"/>	192.168.0.1

Enable VPN Remote Dial In from LAN Selected LAN 

Isolate VPN Users from each other

LAN 2

LAN 3

Note:

1. VPN Remote Dial-In from LAN supports LAN subnets except for LAN1. Please create another LAN before using this function.
2. VPN Remote Dial-In from LAN supports VPN protocols IPsec, SSL, and WireGuard.

Reference:

<https://www.draytek.com/support/knowledge-base/11438>

VPN From LAN

2. Create the VPN profile in VPN and Remote Access >> Remote Dial-in User.

- VPN from LAN function supports SSL VPN, IPsec, and WireGuard VPN protocols
- Ensure the LAN subnet setting should be the server LAN the VPN needs access
- The VPN client will use the assigned IP to access the servers

VPN and Remote Access >> Remote Dial-in User

Index No. 63

<input checked="" type="checkbox"/> Enable this Account <input type="checkbox"/> Multiple Concurrent Connections Allowed Idle Timeout <input type="text" value="0"/> second(s)	User Account and Authentication Username <input type="text" value="autocheck"/> Password <input type="password" value="*****"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) <input type="checkbox"/> Enable Time-based One-time Password(TOTP) <input type="button" value="Regenerate"/>
Allowed Dial-In Type <input type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> IKEv1/IKEv2 <input type="checkbox"/> IKEv2 EAP <input type="checkbox"/> IPsec XAuth <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/> <input type="button" value="v"/> <input type="checkbox"/> SSL Tunnel <input type="checkbox"/> OpenVPN Tunnel <input checked="" type="checkbox"/> WireGuard	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value=""/> Max: 128 characters <input type="checkbox"/> Digital Signature(X.509) None <input type="button" value="v"/>
<input type="checkbox"/> Specify Remote Node Remote Client <input checked="" type="radio"/> IP <input type="radio"/> Domain Name <input type="text" value=""/> or Peer ID <input type="text" value=""/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	IPsec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input type="checkbox"/> AES Local ID (optional) <input type="text" value=""/>
Subnet <input type="text" value="LAN 1"/> <input type="button" value="v"/> <input checked="" type="checkbox"/> Assign Static IP Address <input type="text" value="172.17.5.250"/>	WireGuard Peer Setting <input type="button" value="Client Config Generator"/> Public key <input type="text" value="ssUEvqphHb9evl0/OXejK"/> Pre-shared key <input type="text" value="optional"/> Persistent keepalive <input type="text" value="60"/> second(s)
	Schedule Profile None <input type="button" value="v"/> , None <input type="button" value="v"/> , None <input type="button" value="v"/> , None <input type="button" value="v"/>

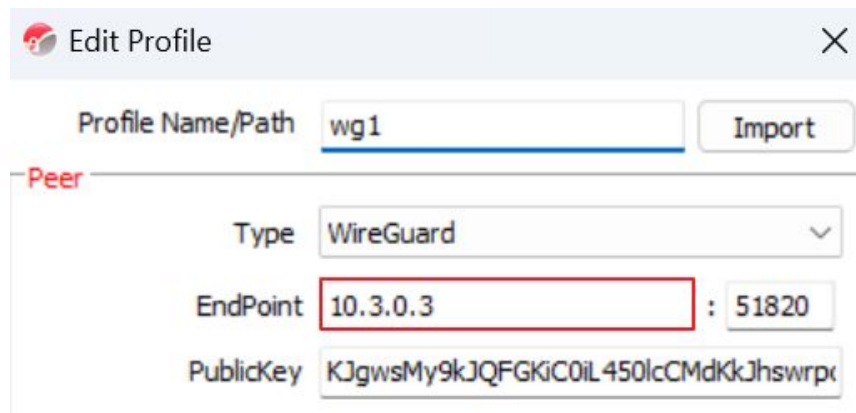
Reference:

<https://www.draytek.com/support/knowledge-base/11438>

VPN From LAN

3. Create new profile on Smart VPN Client

- VPN Server's IP address can be the Router's LAN2 IP or the Router's WAN IP (NAT Loopback)
- ensure the VPN client obtains an IP from LAN2



Edit Profile [Close]

Profile Name/Path:

Peer

Type:

EndPoint: :

PublicKey:




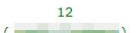
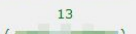
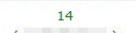
Reference:

<https://www.draytek.com/support/knowledge-base/11438>

VPN From LAN

- We can check the status from VPN and **Remote Access >> Connection Management** page
 - When the VPN comes from LAN, the Remote IP will mark from LAN.

VPN Connection Status

All VPN Status	LAN-to-LAN VPN Status			Remote Dial-in User Status					
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(bps)	UpTime	
11 () Local User Database	WireGuard	 via WAN2 	172.17.5.110/32	73984	240	10012	240	00:08:22	<input type="button" value="Drop"/> <input type="button" value="Detail"/>
12 () Local User Database	WireGuard	10.3.14.2 from LAN	172.17.5.141/32	18971	1.62 K	11063	1.58 K	03:31:30	<input type="button" value="Drop"/> <input type="button" value="Detail"/>
13 () Local User Database	WireGuard	10.3.16.161 from LAN	172.17.5.168/32	21396	32	8389	32	02:25:21	<input type="button" value="Drop"/> <input type="button" value="Detail"/>
14 () Local User Database	WireGuard	10.3.11.157 from LAN	172.17.5.111/32	5534303	0	1267488	0	1 day 01:32:19	<input type="button" value="Drop"/> <input type="button" value="Detail"/>
15 (eason_jhan) Local User Database	WireGuard	10.3.9.10 from LAN	172.17.5.90/32	201590	0	121123	0	1 day 19:56:29	<input type="button" value="Drop"/> <input type="button" value="Detail"/>

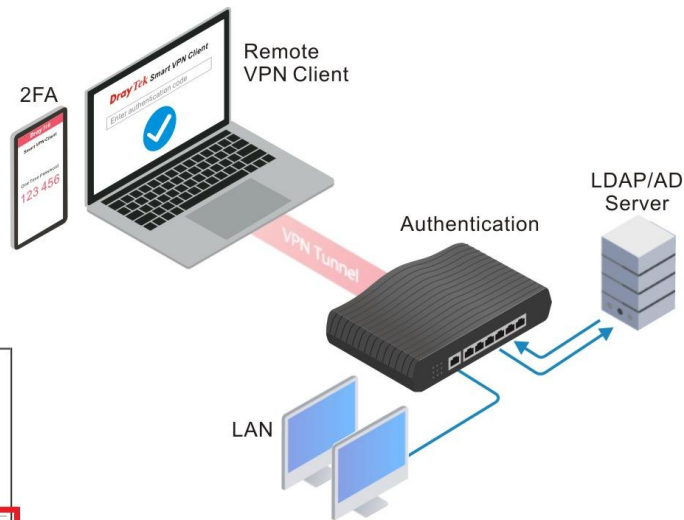
Reference:

<https://www.draytek.com/support/knowledge-base/11438>

VPN 2FA with AD/LDAP Server

DrayTek offers two-factor authentication solution for customer using AD/LDAP to authenticate remote dial-in VPN clients.

It can add extra layer of security for VPN connections, and customer can also benefit from saving the extra cost on SMS messages or license fees for the official authentication system.

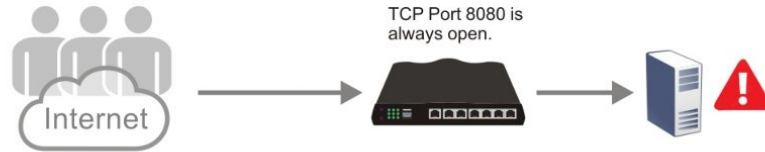


PPP General Setup

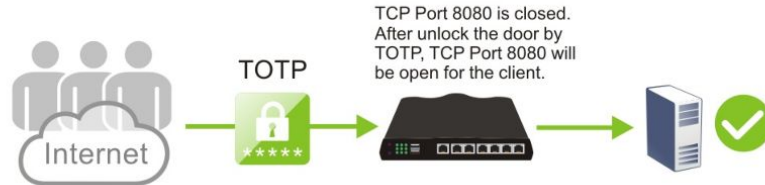
PPP/MP Protocol									
Dial-In PPP Authentication	<input type="text" value="PAP/CHAP/MS-CHAP/MS-CHAPv2"/>								
Dial-In PPP Encryption(MPPE)	<input type="text" value="Optional MPPE"/>								
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No								
Username	<input type="text" value="Max: 128 characters"/>								
Password	<input type="text" value="Max: 128 characters"/>								
IP Address Assignment for Dial-In Users when DHCP is disabled.									
	<table border="1"><thead><tr><th>Start IP Address</th><th>IP Pool Counts</th></tr></thead><tbody><tr><td>LAN 1</td><td><input type="text" value="192.168.121.200"/> <input type="text" value="50"/></td></tr><tr><td>LAN 2</td><td><input type="text" value="192.168.222.200"/> <input type="text" value="50"/></td></tr><tr><td>LAN 3</td><td><input type="text" value="10.10.3.200"/> <input type="text" value="50"/></td></tr></tbody></table>	Start IP Address	IP Pool Counts	LAN 1	<input type="text" value="192.168.121.200"/> <input type="text" value="50"/>	LAN 2	<input type="text" value="192.168.222.200"/> <input type="text" value="50"/>	LAN 3	<input type="text" value="10.10.3.200"/> <input type="text" value="50"/>
Start IP Address	IP Pool Counts								
LAN 1	<input type="text" value="192.168.121.200"/> <input type="text" value="50"/>								
LAN 2	<input type="text" value="192.168.222.200"/> <input type="text" value="50"/>								
LAN 3	<input type="text" value="10.10.3.200"/> <input type="text" value="50"/>								
PPP Authentication Methods									
<input checked="" type="checkbox"/> Remote Dial-in User									
<input checked="" type="checkbox"/> RADIUS									
<input checked="" type="checkbox"/> AD/LDAP									
LDAP Profile									
<input checked="" type="checkbox"/> TACACS+									
VPN Two-Factor Authentication for AD/ LDAP									
<input type="checkbox"/> Authentication Code via Email									
Email Object <input type="text" value="1 - hinet"/>									
<input type="checkbox"/> Authentication Code via SMS									
SMS Object <input type="text" value="1 - ???"/>									
<input checked="" type="checkbox"/> Time-based One-time Password (TOTP)									
<input checked="" type="checkbox"/> LDAP Attribute for TOTP Secret: <input type="text" value="pager"/>									
<input type="checkbox"/> Shared Secret: <input type="text" value="All users share this Secret"/>									
<input type="button" value="Regenerate"/> <input type="button" value="Copy"/>									

Port Knocking

Typical NAT Port Redirection



NAT Port Knocking



Configuring NAT Port Redirection rules is the typical way to allow the internal servers to be accessible from the Internet. However, once the port opens, it is exposed to the Internet and can be scanned by the malware.

Port knocking is a technology that can add an extra layer of protection to the internal servers. Its basic idea is that only open ports are at risk of being attacked, so it allows all ports to be closed at the beginning. Do not open them, and then set a password based on the port combination. Only those who know the password can open the ports and connect.

Server Load Balancing

Hosting multiple servers to share the traffic load for the same service is common. It can avoid excessive load on a single server by distributing the load, optimizing resource usage, and preventing a single server failure.

With Server Load Balance, when massive connections enter the router, the router will distribute the inbound NAT sessions among the servers with the configured load balance weight.



Smart Action

- **Event** → **Action**, predefined event triggers predefined action
- WUI browse through
- Web Notification
- **Log** Keyword Match (**syslog** log, **console** log, **suricata** log, see linux “application > log collector”)

Smart Action

DrayTek Network Security Overview



Network Security - Actions to Improve Security

1. Use latest firmware - *Very Important*
2. Change the Default Admin Password
3. Use ACL - Access List for remote access - Use HTTPS - Use different port eg 8443.
4. If the VPN service is enabled, use the access list feature or specify the VPN peer IP to restrict VPN access.
5. Enable activation code - CAPTCHA.
6. Enable 2 Factor Activation login - ACS2/3.
7. Change Management Ports.
8. Brute Force protection - DOS attack in System Maintenance.
9. Use Firewall DOS Defense - Spoofing Defense - use Blacklist - Web content filter
10. Restricted access to the Management console.
11. Disable unused features such as unused VPNs.
12. **Capture and check the syslog regularly.**
13. Use a secure password for admin login and all VPN profiles. Change the password often. Longer passwords are better >12 chars
14. Consider to use 2 Factor Authentication for web or MOTP for VPN login.
15. Re-sign and Change the default security certificates for SSL or HTTPS access.
16. Enable Suricata in the Vigor3912s Router

Workshop Manual Page 11

let “smart action”
do the checkings

Smart Action

DrayTek Network Security Overview



Cyberattack as shown in syslog

Example of attempted VPN login from the Internet

This attack comes from IP: 146.88.240.4 which is from a US company, <https://www.netscout.com/arbor-ddos>. This IP address appeared in similar Routers in other parts of the country.

Here are the logs of VPN dial-in failure often received:

```
2021-07-02_02:55:12.16511 [L2TP][@146.88.240.4] pppShutdown
2021-07-02_02:55:25.17257 [L2TP][Radius/LDAP][0:vpn][@146.88.240.4] maximum retries exceed
2021-07-02_02:55:25.18220 [L2TP][@146.88.240.4] pppShutdown
2021-07-02_02:55:35.69281 [L2TP][Radius/LDAP][0:vpn][@146.88.240.4] maximum retries exceed
2021-07-02_02:55:35.70141 [L2TP][@146.88.240.4] pppShutdown
2021-07-02_02:56:04.76506 [L2TP][Radius/LDAP][0:vpn][@146.88.240.4] maximum retries exceed
2021-07-02_02:56:04.76995 [L2TP][@146.88.240.4] pppShutdown
```

Workshop Manual Page 20

use “smart action” to
notify admin of similar attacks

Smart Action

Applications >> Smart Action

User Defined Profile Index : 3

Enable

Comment: attempted VPN login from the Internet

Event Category: System

Event Type: Log Keyword Match

Keyword:
maximum retries exceed

Keyword Type: TEXT

Count: 1


Timespan: 0 seconds

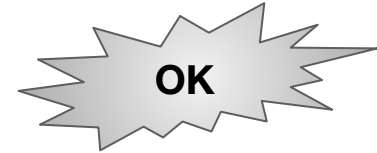
Facility: ALL

Level: INFO(6)

Action Category: System

Action Type: Web Notification

Message: 
##KW_MSG##



Get Web Notification

URL Reputation

URL Reputation is a cloud-based technology to provide Threat Intelligence Service. This service adds an extra layer of security protection to LAN client for their online activities.

There are 82 categories in total, 10 of which are security-focused, providing comprehensive and up-to-date protection to your home network or office network.

The various categories cover network security, including malware, spyware, adware, parental control for child protection, business, social networking, and more to ensure a safe online environment while also boosting employee productivity and can reach efficient bandwidth management.

You can purchase URL reputation S card for your Vigor3912.



CSM >> Web Content Filter Profile

Profile Index: 1
Profile Name: Log

Black/White List
 Enable
Action: URL keywords:

Action:

Security

 Bot Nets DNS Over HTTPS Hacking
 Keyloggers and Monitoring Malware Sites Parked Domains
 Phishing and other Frauds Proxy Avoidance and Anonymizers SPAM URLs
 Spyware and Adware

Parental Control

 Abortion Abused Drugs Adult and Pornography
 Alcohol and Tobacco Cheating Cult and Occult
 Gross Hate and Racism Illegal
 Low-THC Cannabis Products Marijuana Nudity
 Questionable Self Harm Sex Education
 Swimsuits and Intimate Apparel Violence Weapons

Productivity

 Auctions Computer and Internet Info Content Delivery Networks
 Dating Gambling Games
 Home and Garden Hunting and Fishing Image and Video Search
 Individual Stock Advice and Tools Internet Communications Job Search
 Motor Vehicles Music Pay to Surf
 Peer to Peer Personal Storage Real Estate
 Shareware and Freeware Shopping Social Networking
 Sports Streaming Media Training and Tools
 Web Advertisements Web Hosting

General Use

 Business and Economy Computer and Internet Security Dead sites
 Dynamically Generated Content Educational Institutions Entertainment and Arts
 Fashion and Beauty Financial Services Government
 Health and Medicine Internet Portals Kids
 Legal Local Information Military
 News and Media Online Greeting Cards Personal Sites and Blogs
 Philosophy and Political Advocacy Recreation and Hobbies Reference and Research
 Religion Search Engines Society
 Translation Travel Web-based Email
 Uncategorized Sites

IP Reputation

01-20 High Risk



These are high risk IP addresses. There is a high predictive risk that these IPs will deliver attacks – such as malicious payloads, DoS attacks, or others – to your infrastructure and endpoints.

21-40 Suspicious



These are suspicious IPs. There is a higher than average predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.

41-60 Moderate Risk



These are generally benign IPs but have exhibited some potential risk characteristics. There is some predictive risk that these IPs will deliver attacks to your infrastructure and endpoints.

61-80 Low Risk



These are benign IPs and rarely exhibit characteristics that expose your infrastructure and endpoints to security risks. There is a low predictive risk of attack.

81-100 Trustworthy



These are clean IPs that have not been tied to a security risk. There is very low predictive risk that your infrastructure and endpoints will be exposed to attack.

every IP has a score or **reputation** given by **BrightCloud**



IP Reputation



Home

Look up URL or IP:

我不是機器人



reCAPTCHA
隱私權 · 條款

LOOK UP



WWW.DRAYTEK.COM

Web Reputation:



- Trustworthy (88 of 100)

[Request a reputation change](#)

IP Reputation

https://www.brightcloud.com/tools/url-ip-lookup.php



Look up URL or IP:

我不是機器人



LOOK UP

If you have a mutually executed agreement with Webroot, those terms apply to your use of the BrightCloud Service. If you do not have a mutually executed agreement with Webroot, by clicking "LOOK UP", you agree to the terms and conditions of the [BrightCloud Threat Intelligence Service for Enterprise Agreement](#).

Request a Change:

URL or IP: *

Optional: [I would like to suggest a category for this URL](#)

Your email: *



PROFTRAFFICCOUNTER.COM

Web Reputation:



- High Risk (10 of 100)

[Request a reputation change](#)

Web Category:

- Malware Sites

[Request a category change](#)

Web Reputation Influences:

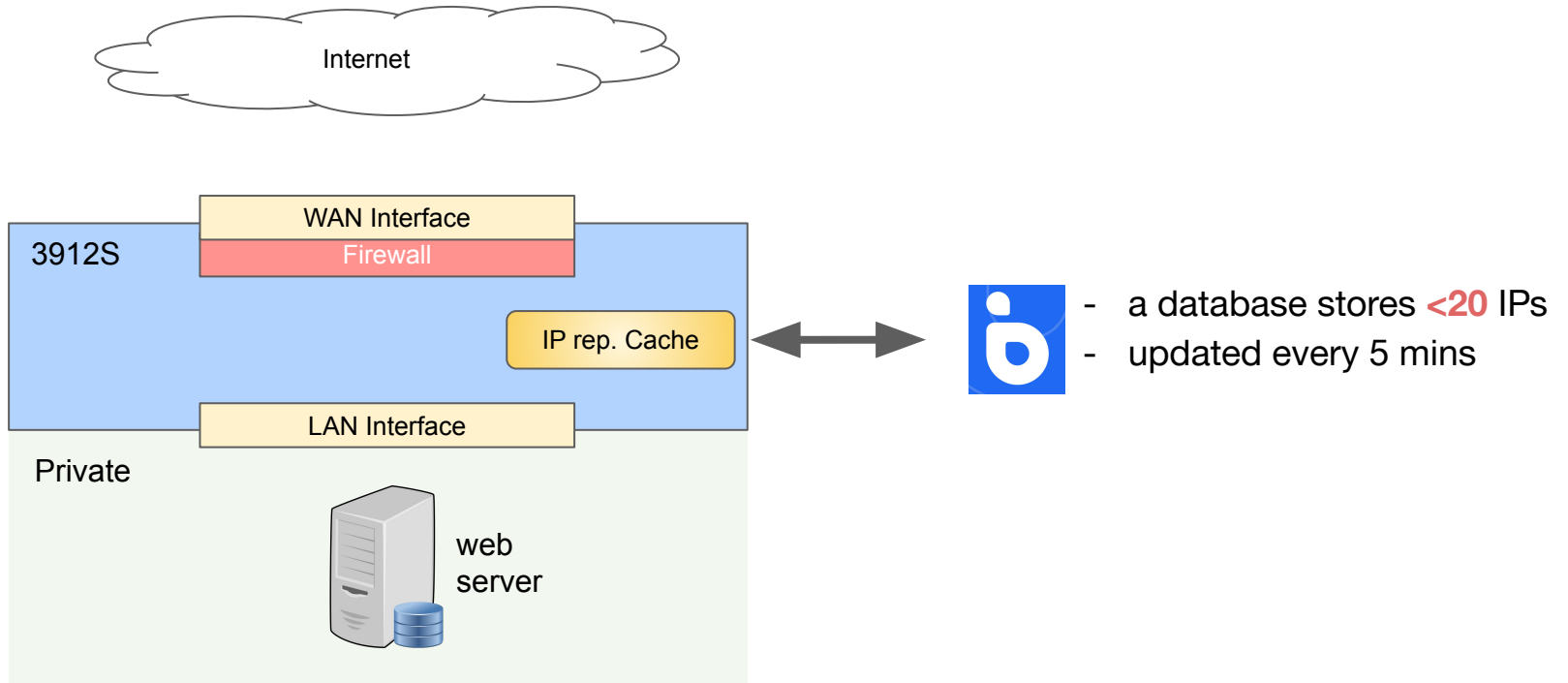
- 1 infections (past 12 months)
- Low popularity
- 1 months old (not established)

Impact:

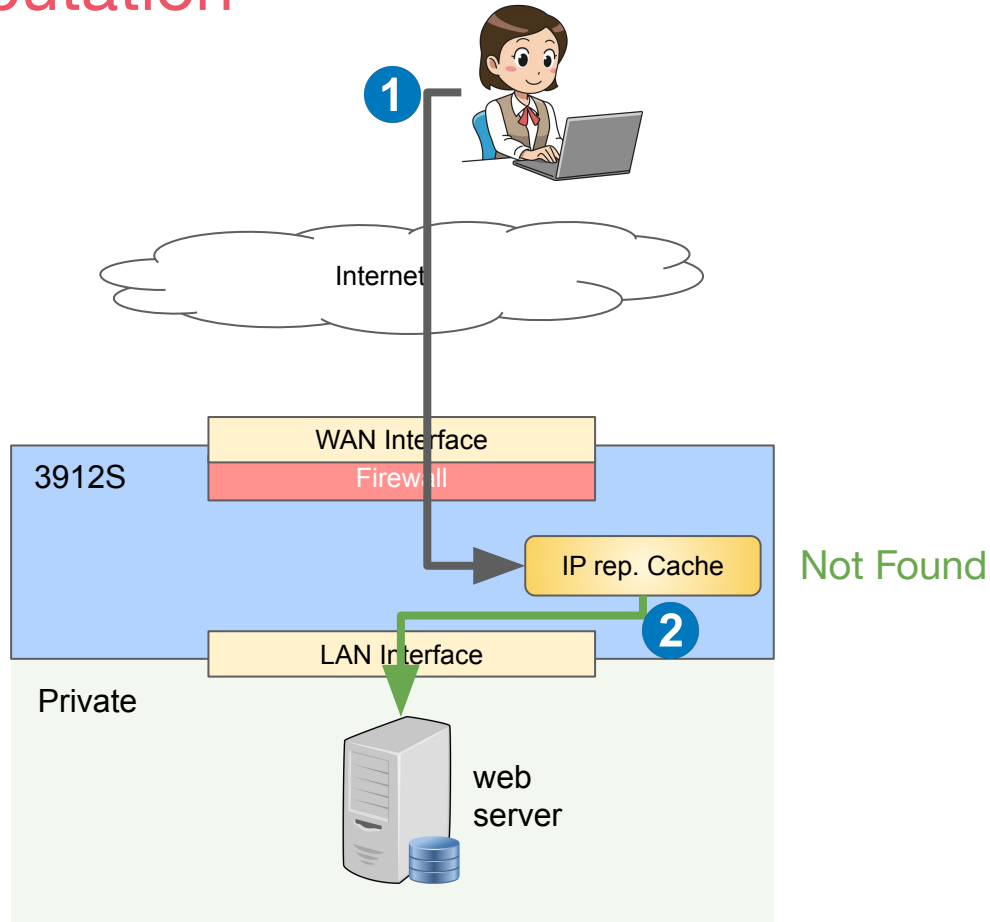


Web Database Version: 8.921 - Last Updated: 04/13/2024 21:04:02 UTC

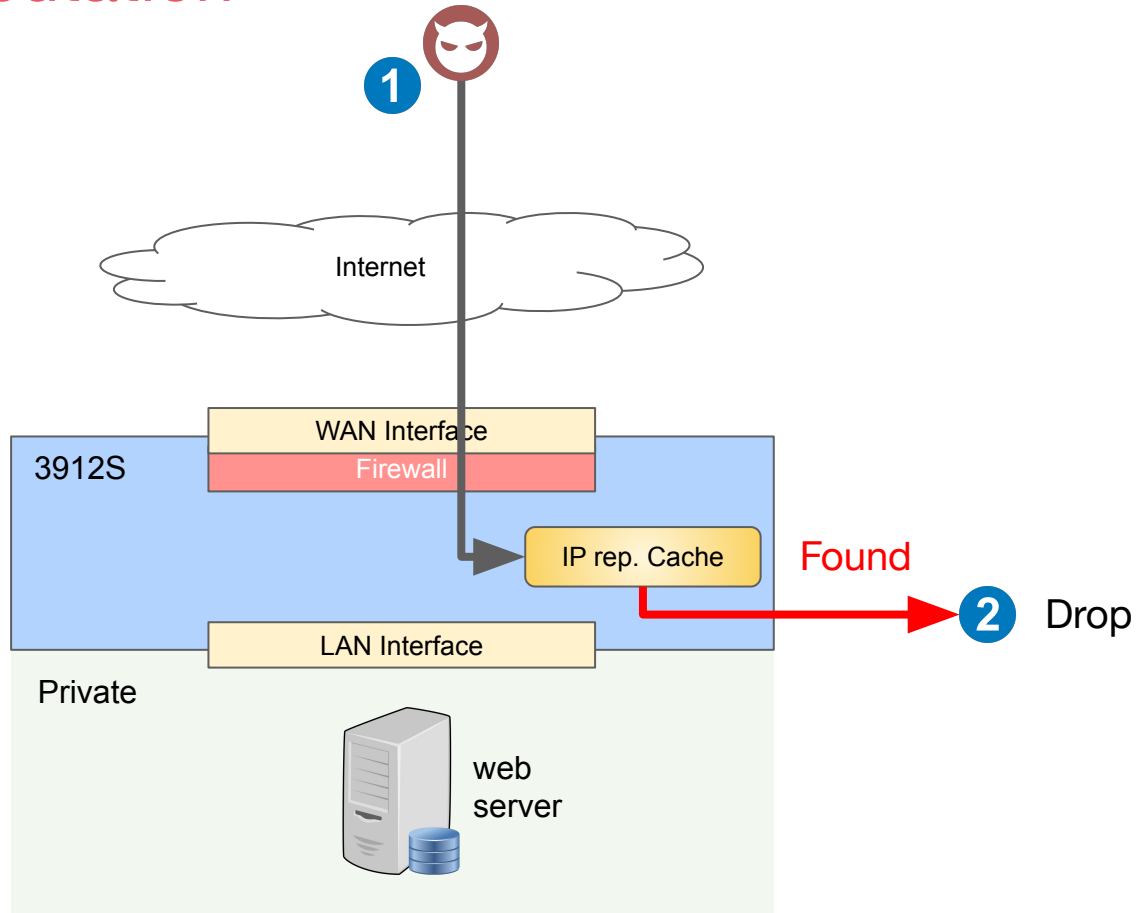
IP Reputation



IP Reputation



IP Reputation



IP Reputation

Firewall >> Defense Setup

DoS Defense	Spoofing Defense	IP Reputation Defense
-------------	------------------	-----------------------

Web-Filter License

[Status : **Inactivated**]

Please activate license in Web Content Filter page.

Enable function

Log:

- Block Internet IPs with Bad IP Reputation from accessing Vigor Router
- Block Internet IPs with Bad IP Reputation from accessing LAN Hosts

Advanced Setting :

Cache Size : (256KB memory)

Cache Timeout :

OK

[RD3FT_3912S]2024-04-15 15:27:28 [IP Reputation] 162.142.125.84
reputation=11 threat=Windows Exploit try access proto:1

下午 03:27

[RD3FT_3912S]2024-04-15 15:27:31 [IP Reputation] 162.142.125.84
reputation=11 threat=Windows Exploit try access proto:1

下午 03:27

[RD3FT_3912S]2024-04-15 15:27:32 [IP Reputation] 162.142.125.14
reputation=9 threat=Spam Source try access proto:17 local port:
500

下午 03:27

[RD3FT_3912S]2024-04-15 15:27:35 [IP Reputation] 162.142.125.14
reputation=9 threat=Spam Source try access proto:1

下午 03:27

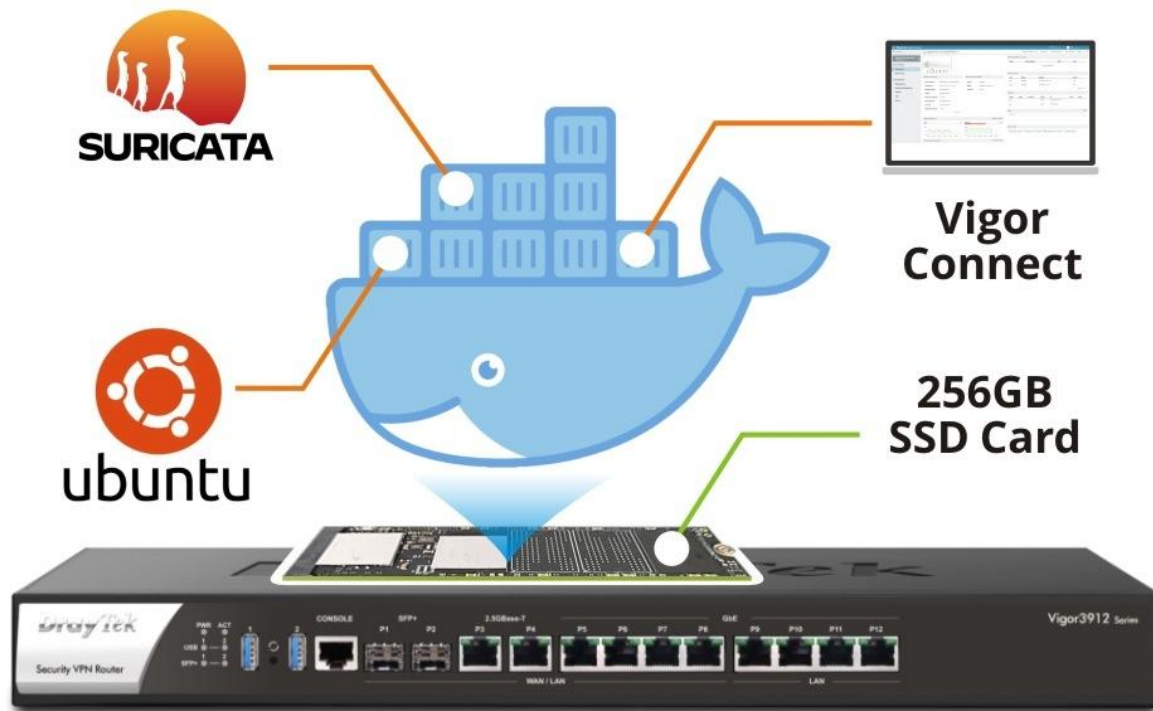
[RD3FT_3912S]2024-04-15 15:27:36 [IP Reputation] 162.142.125.84
reputation=11 threat=Windows Exploit try access proto:1

下午 03:27

applies to **inbound** traffic only

SSD Application 3912S Only

- Suricata
- Vigor Connect
- Do Anything you can do on Ubuntu



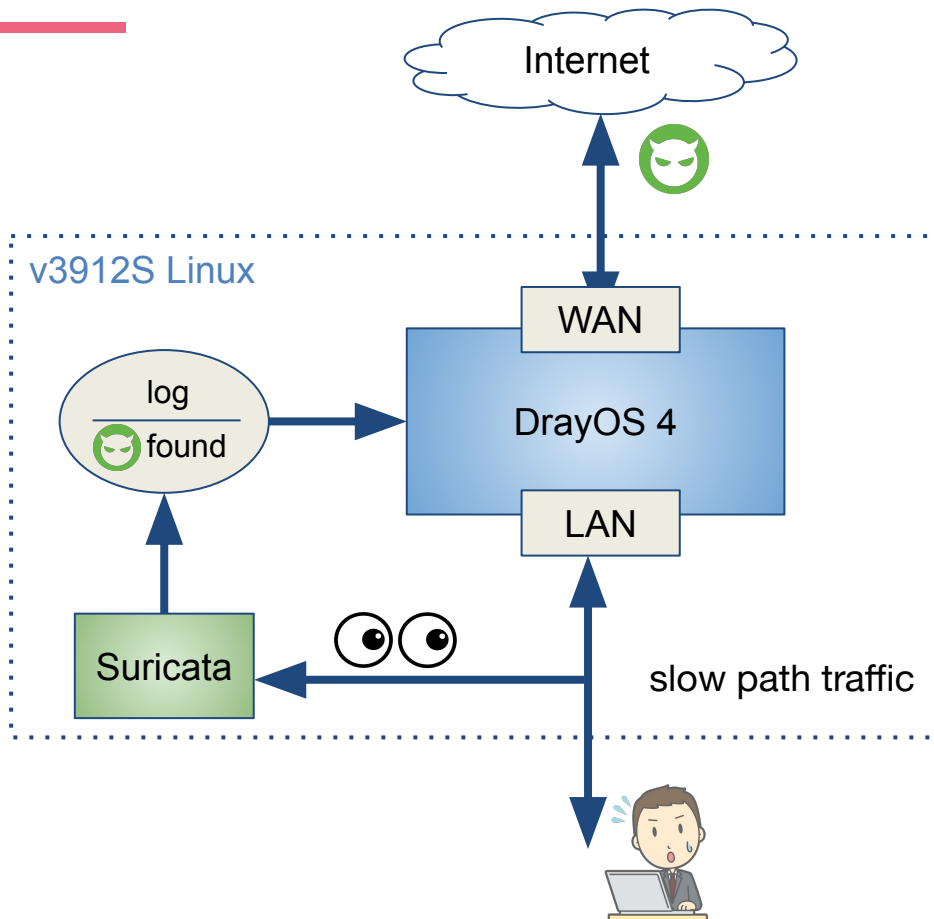
Key Feature Suricata



Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

Suricata is an open-source threat detection system. It supports more than 60000 rules, including 6000+ CVE rules, and can detect and prevent a **wide range of network threats**, such as malware, network intrusions, denial-of-service attacks, and data breaches. Vigor3912S supports **Linux Applications with Docker**, which can install this powerful software inside and use it to protect the network.

Suricata's Role and Topology



Suricata Role:

- Monitoring
(all traffic to/from LAN host)
- Alert
- **Entry-Level IDS**

Suricata Basics

Linux Applications >> Suricata

General Setup Statistics

General Setup ?

- Enable ?
- Suricata Core Auto Update
- Suricata Rule Auto Update

Restart Suricata

Suricata software version

Core Base: v3912-r2 ?
Core Status: running
Core Version: v3912-r2-20240222152515
Core Last Updated: 2024-04-09T15:50:24
Rule Last Updated: 2024-04-10T06:32:18
Rule Last Changed: 2024-04-10T06:32:18

Suricata signature version

Rule Setup (classtype) ?

Select/Clear All (1)

Select/Clear All (2)

Select/Clear All (3)

Select/Clear All (4)

Misc Activities

Select/Clear All

- Not Suspicious Traffic (3)
- A TCP connection was detected (4)
- Generic Protocol Command Decode (3)
- Generic ICMP event (3)
- Attempted Information Leak (2)
- Information Leak (2)
- Large Scale Information Leak (2)
- Attempted User Privilege Gain (1)
- Unsuccessful User Privilege Gain (1)
- Successful User Privilege Gain (1)

auto checking for the latest update once per day

Suricata Basics

Linux Applications >> Suricata

General Setup ? **Statistics**

General Setup ?

Enable ?

Suricata Core Auto Update

Suricata Rule Auto Update

Core Base: v3912-r2 ?

Core Status: **running**

Core Version: v3912-r2-20240222152515

Core Last Updated: 2024-04-09T15:50:24

Rule Last Updated: 2024-04-10T06:32:18

Rule Last Changed: 2024-04-10T06:32:18

higher severity ← **lower severity**

Select/Clear All (1) Select/Clear All (2) Select/Clear All (3) Select/Clear All (4)

Misc Activities

- Not Suspicious Traffic (3)
- A TCP connection was detected (4)
- Generic Protocol Command Decode (3)
- Generic ICMP event (3)
- Attempted Information Leak (2)
- Information Leak (2)
- Large Scale Information Leak (2)
- Attempted User Privilege Gain (1)
- Unsuccessful User Privilege Gain (1)
- Successful User Privilege Gain (1)

specify the type of threat you want to keep an eye on


Suricata Basics

Network Trojan and Malware Activities

Select/Clear All

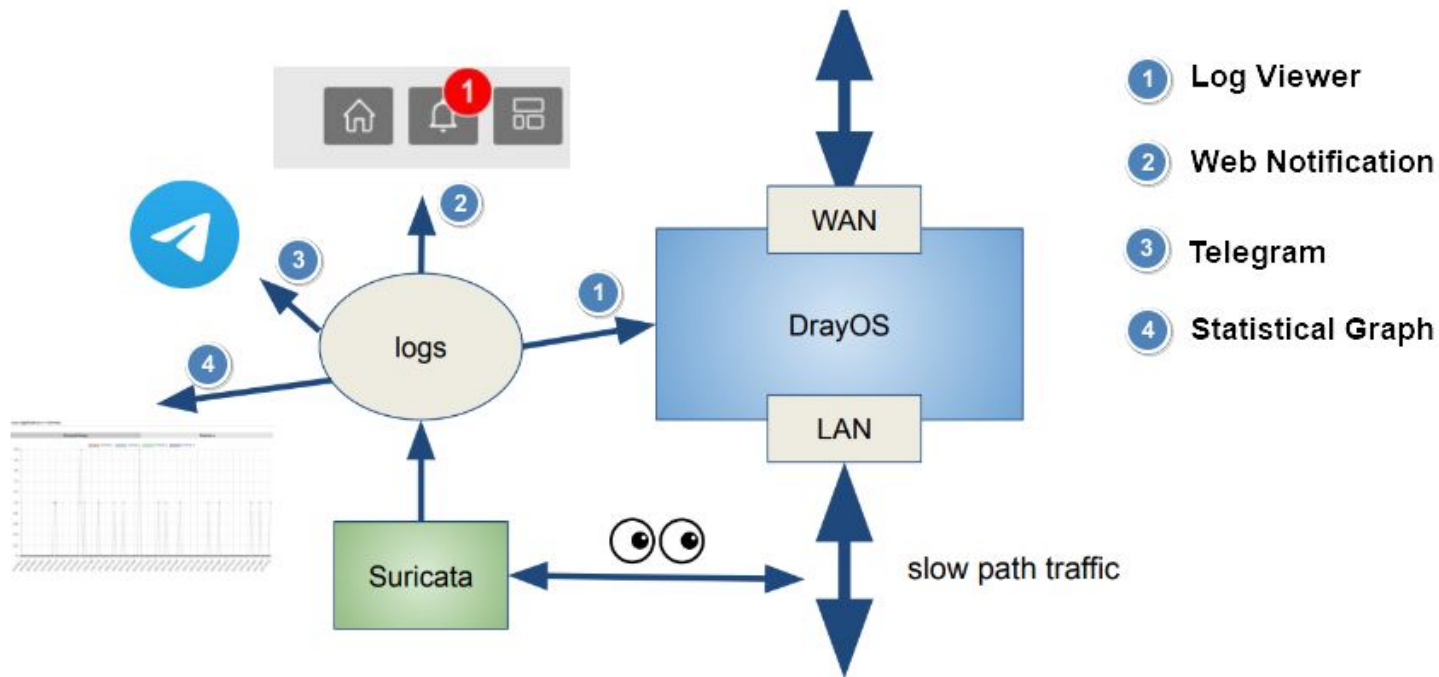
- A Network Trojan was detected (1)
- access to a potentially vulnerable web application (2)
- Web Application Attack (1)
- Targeted Malicious Activity was Detected (1)
- Exploit Kit Activity Detected (1)
- Domain Observed Used for C2 Detected (1)
- Malware Command and Control Activity Detected (1)

Log Setup

1. Suricata logs can be viewed from "**Linux Applications > Log Collector**" (facility: suricata)
2. Specific Suricata logs can be configured to notify "Web Notification" or "Telegram" using "**Applications > Smart Action**" 

use in conjunction with “smart action”
for maximising its potential

Suricata Notification Actions



Suricata Web Notification

The screenshot shows the Suricata configuration interface. On the left, the 'Smart Action' configuration is visible, with 'Web Notification' selected as the 'Action Type'. The configuration includes fields for 'Comment', 'Event Category', 'Event Type', 'Keyword', 'Keyword Type', 'Count', 'Timespan', 'Facility', 'Level', 'Action Category', and 'Action Type'. The 'Block the following if present' section has checkboxes for 'First IP', 'Second IP', and 'LAN'. On the right, a 'Web Notification' window displays a list of log entries with their timestamps, classifications, and action profiles. An orange arrow points to the notification bell icon in the top navigation bar.

Save you the trouble of manually browsing through all the logs

Can detect the network threats and **automatically block IP** that matched to some keywords by **Smart Action**

Can **block unknown IP** manually and add it to BFP table .

The screenshot shows the 'Brute Force Protection: Blocked IP List' table and the 'Web Notification' window. The table has columns for Index, IP Address, FTP, HTTP, HTTPS, TELNET, and TROJAN. The 'Web Notification' window displays log entries with their timestamps, classifications, and action profiles.

Index	IP Address	FTP	HTTP	HTTPS	TELNET	TROJAN
1	111.249.97.104					

Showing 1 to 1 of 1 entries

Suricata Telegram

Applications >> Smart Action

Profile Index : 4

Enable

Comment:

Event Category:

Event Type:

- Schedule
- Date and Time
- CPU Usage
- Memory Usage
- Log Keyword Match (user-defined)**
- Log Keyword Match (inbuilt)
- Session Usage

Count:

Timespan: seconds

Facility:

Level:

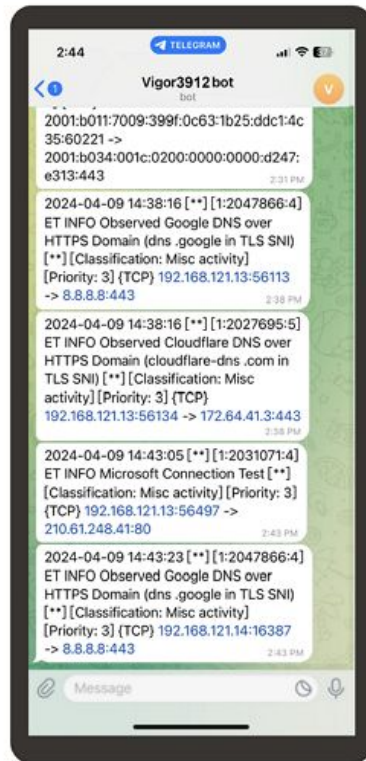
Action Category:

Action Type:

Server URL:

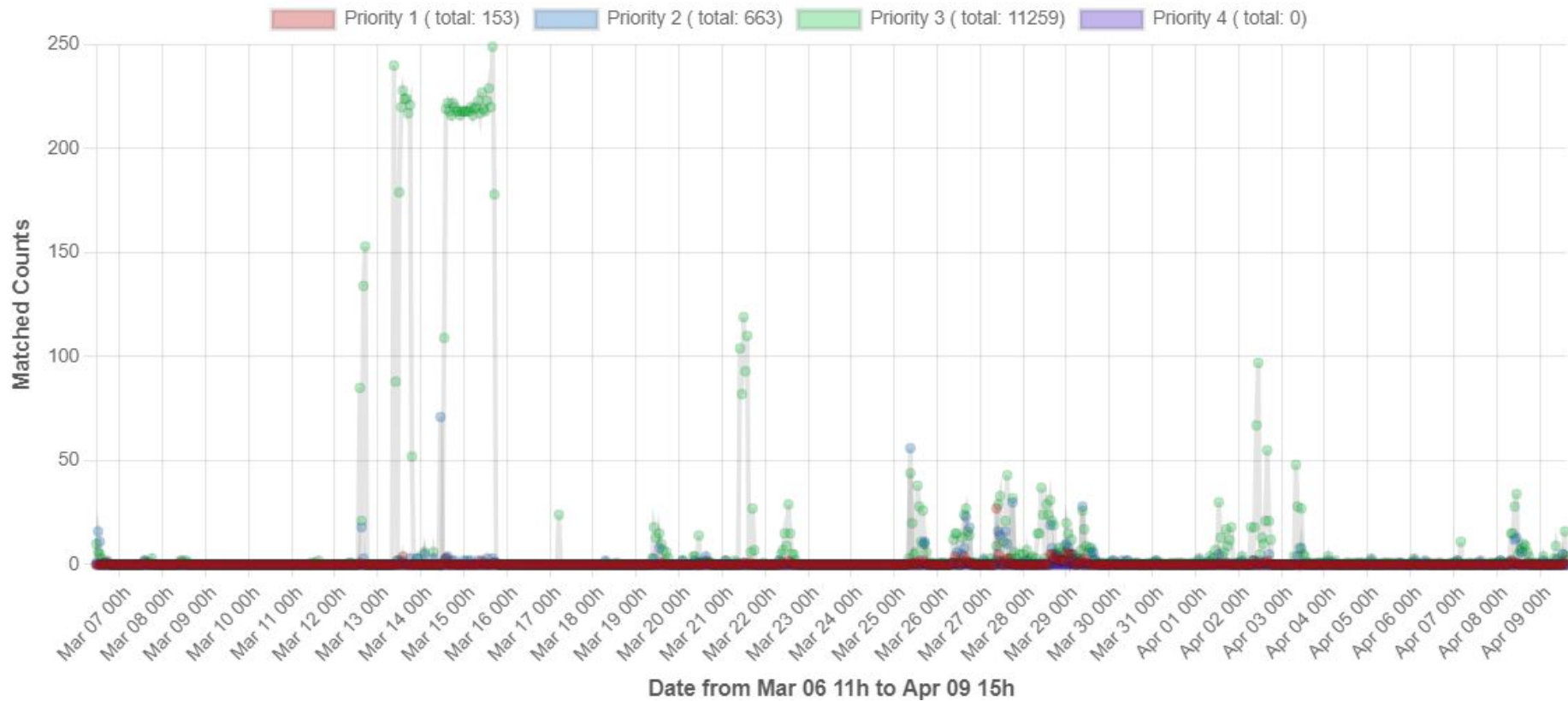
POST Content: 

```
{
  "chat_id": "",
  "text": "##KW_MSG##"
}
```



Suricata Statistical Graph

Suricata Statistics







New Products

- DrayOS 5 Router
- Vigor1100_v2 series
- Vigor2136 series

Vigor1100_v2 series



1x GPON WAN

4x GbE LAN

1x configurable backup WAN

1x USB 3.0

Wireless

2x2, 2.4GHz, 802.11b/g/n/ax, 574 Mbps

3x3, 5GHz, 802.11 a/n/ac/ax, 2402 Mbps

Optional Feature - VoIP

Vigor2136 series



IPsec / OpenVPN / Wireguard VPN

Up to 4 VPN Tunnels

1x 2.5 GbE WAN

1x 2.5 GbE Switchable WAN/LAN

3x GbE LAN

2x USB 2.0

Wireless

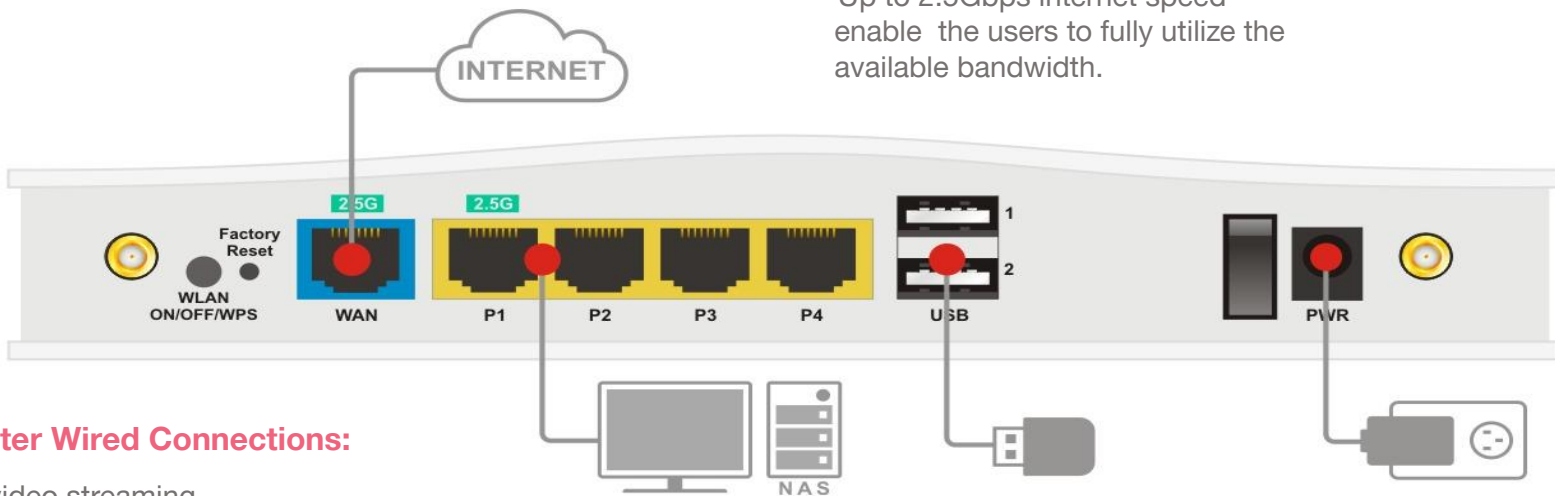
2x2, 2.4GHz, 802.11b/g/n/ax, 574 Mbps

2x2, 5GHz, 802.11 a/n/ac/ax, 2402 Mbps

Multi-Gig Router

Beyond Gigabit

Up to 2.5Gbps internet speed enable the users to fully utilize the available bandwidth.

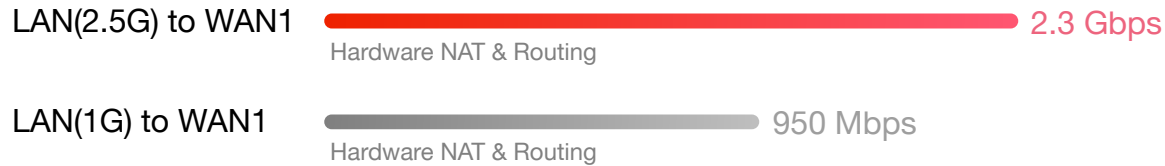


Faster Wired Connections:

- 4K video streaming,
- online gaming,
- large file transfers
- network-attached storage (NAS) devices etc.

Hardware NAT & Routing

With acceleration enabled, Vigor2136's NAT throughput can reach 2.3Gbps , while still meeting high expectation of QoS quality. You may easily prioritized business critical apps, and always keep VoIP in 1st priority.



Vigor2136 support the most secure VPN protocols



Vigor2136 Series

	Vigor2136	Vigor2136ax	Vigor2136Vax	Vigor2136FVax
Description	General Model	Wireless Model	VoIP & Wireless Model	VoIP & Wireless Model With Fiber WAN
Fixed WAN		1 X 2.5GbE RJ-45		SFP Slot(Project base)
Fixed LAN		1 x 2.5GbE RJ-45, 3x GbE RJ-45		
USB Port		2 x USB 2.0		
VoIP Gateway	×	×	✓	
FXS Port	×	×	2 x RJ-11 (Project base)	
Antenna	×	2 x Dual-band Detachable (2.3 dBi) + 1 x Internal Antenna (PIFA) for 5GHz (3.5 dBi)		
2.4G WLAN	×	2T2R, 802.11b/g/n/ax		
2.4G WLAN Max. Link Rate	×	574 Mbps		
5G WLAN	×	3T3R (2ss), 802.11a/n/ac/ax		
5G WLAN Max. Link Rate	×	2402 Mbps		

Vigor2136 2.5G Router with AX3000 Capacity

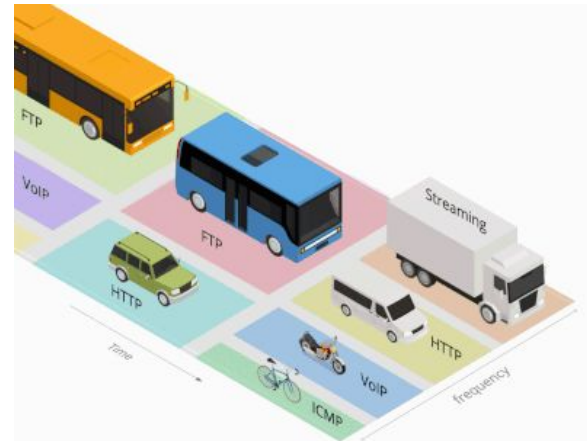


The V2136ax is a 2x2 dual-band Wi-Fi router that provides 160MHz bandwidth and 1024-QAM to greatly increase the speed of wireless connection. The theoretical speed is up to 3000Mbps, of which 574Mbps is in the 2.4GHz band and 2402Mbps in the 5GHz band. Which is 2.5 times faster than an 802.11ac 2x2 dual-band router.

In the household. It's also equipped with business-grade features, including URL Reputation, Route Policy, App-based QoS and lots more, and is perfect for professional smart homes/SOHO users who would like to take full control of their own network.

OFDMA splits a single transmission into groups of subcarriers, and each subcarrier can be used by different client. With multiple clients transmitting simultaneously in the same channel, it improves efficiency of every single transmission opportunity.

Imagine **MU-MIMO** is similar to multiple trucks serving users simultaneously. It increases capacity and results in higher speed per users.



Vigor2136 2.5G Router with AX3000 Capacity

Basic Service Set (BSS) forms an ad hoc self-contained network with station-to-station traffic flowing directly, receiving data transmitted by another station, and only filtering traffic based on the MAC address of the receiver.

BSS coloring is a technique used to improve co-existence of overlapping BSSs and to allow spatial reuse within one channel .Simply say BSS coloring helps in mitigating problem of co-channel interference found in legacy wifi networks.

TWT (Target wake time) ensures that end devices spend more time in standby while sending and receiving data more economically. This reduces energy consumption and increases overall efficiency within the home network.It allows an AP to manage activity in the Wi-Fi network, in order to minimize medium contention between Stations (STAs), and to reduce the required amount of time that an STA in the power-save mode needs to be awake.

WPA3 is the latest security protocol designed to safeguard your Wi-Fi traffic. You can enjoy the highest security standard without compromising on wireless performance.

802.11ax feature overview

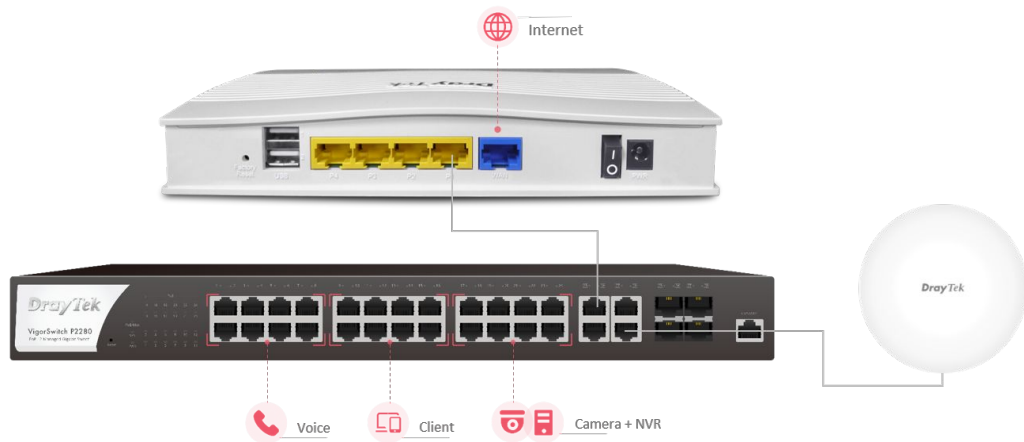
Capabilities	802.11n	802.11ac	802.11ax
Physical Layer (PHY)	High Throughput (HT)	Very High Throughput (VHT)	High-Efficiency Wireless (HEW)
Operating Bands	2.4 and 5 GHz	5 GHz only	2.4 and 5 GHz
MU-MIMO	N/A	DL MU-MIMO only	DL and UL MU-MIMO
Channel Width	20, 40, 80 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
Spread Spectrum Technology	OFDM	OFDM	OFDM, OFDMA
Frequency Modulation	64 QAM	256 QAM	1024 QAM
Power Save	STBC, U-APSD	STBC, U-APSD	STBC, U-APSD, TWT
Spectral Efficiency	N/A	N/A	BSS Coloring (reduce interference)

Virtual AP / Switch Controller

An all-in-one management platform for Vigor devices on the LAN side including 9 APs and 5 Switches

Automatic Device Discovery

All you need is connect the Vigor Switch/AP to the LAN side of the router, Vigor Router will then discover the devices to be managed.



Provisioning

Basic settings may be done on the Vigor Router, and provision to the managed Vigor Switch/AP.

Monitoring

Vigor Router provides a centralized view of managing devices, you may always check if the managed Vigor Switch/AP is online.

System Maintenance

You may perform a factory reset, save/restore a configuration backup, or trigger a remote reboot directly on the Vigor Router. There's no need to log in to each device's management page.

DrayOS5 Identity and Access Management

Vigor2136ax is with DrayOS 5 OS. It's Zero Trust ready.

Precise Device Authentication

Using each device's unique IP and MAC address provides a strong basis for device identification and authentication.

Reduced False Positives

Using IP and MAC addresses reduces the likelihood of legitimate devices being blocked due to other potential factors.

Holistic Security

Combining user ,device, and session-based policies enhances overall security without relying solely on one aspect.

Enhanced Incident Response

When security incidents occurs, you can quickly pinpoint the devices involved and take appropriate actions.

DrayOS5 / IAM

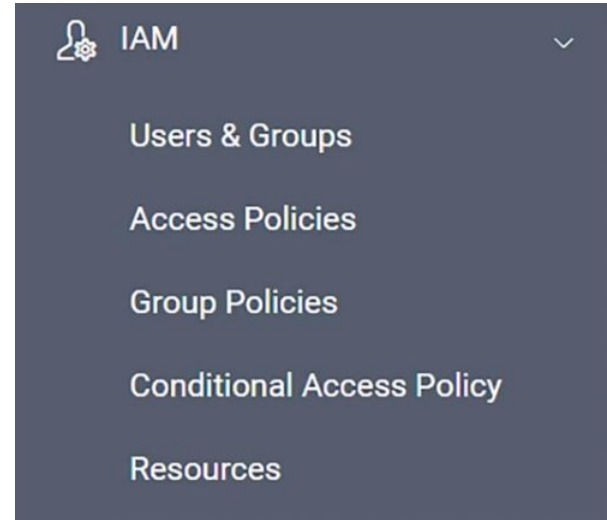
Menu >> IAM

IAM (Identity and Access Management) brings a suite of powerful security enhancements to DrayTek Routers

- Ability to control user privileges
- Define access policies
- Coordinate group policies with the firewall and traffic shaping settings

Menu >> IAM>> Users & Groups

- User account >> user groups makes it easy to control and manage accounts in a group level
- Configure external authentication server
- Enable user and MFA protection



DrayOS5 / IAM

Menu >> IAM>>Access Policies

System administrators can create access policies on the local users in this tab

The access policies can be created according to:

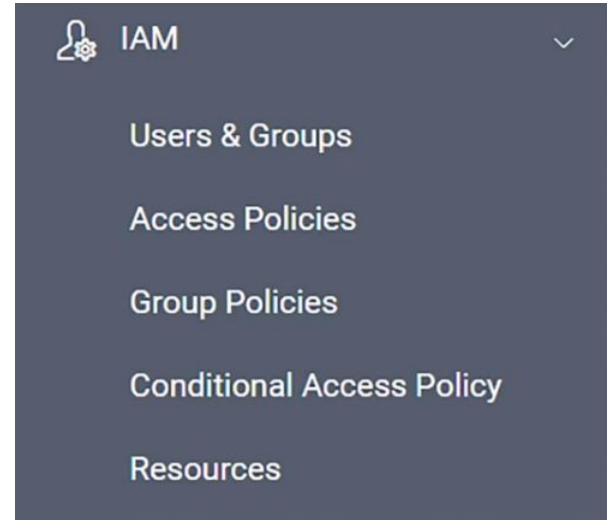
- MAC address filter list
- The allowed /blocked user list
- The login sessions lifetime

Combine these access policies can create a robust security framework for your system.

Menu >> IAM>>Group Policies

Setup group policies with predefined local resources like employees, workstations, network printers, and local servers.

Customise firewall policies and traffic shaping policies to enhance network security and optimize traffic flow.



DrayOS5 / IAM

Menu >> IAM >> Conditional Access Policy

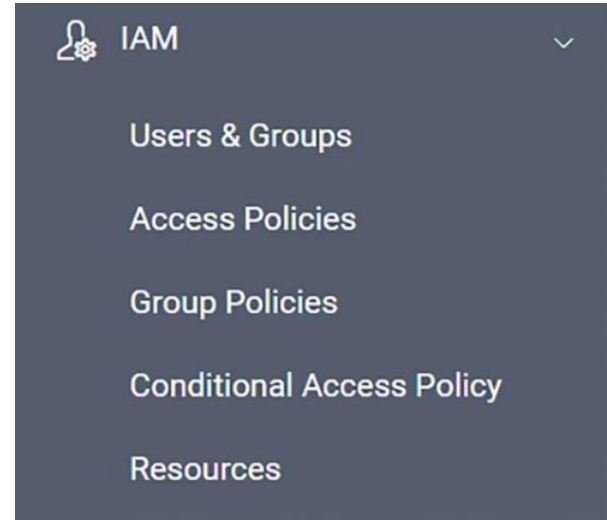
Conditional access policies can require users to provide multiple forms of authentication before they are granted access to a resource.

- Specify a time period for user to re-authenticate
- Restrict access to specific source IP address or ranges of IP addresses
- Specify VLAN-based access controls in your conditional policies
- Set up time schedules when user are allowed to log-in

Menu >> IAM>>Resources

Record local resources' IP addresses and Mac addresses under Resources tab

For examples, Workstations ,Net printers ,PBX systems, NVR systems and servers.



Add-on Business-grade features and applications



URL Reputation

URL Reputation is a cloud-based technology to provide Threat Intelligence Service. This service adds an extra layer of security protection to LAN client for their online activities. There are 82 categories in total, 10 of which are security-focused, providing comprehensive and up-to-date protection to your home network or office network.

The various categories cover network security, including malware, spyware, adware, parental control for child protection, business, social networking, and more to ensure a safe online environment while also boosting employee productivity and can reach efficient bandwidth management.

You can purchase URL reputation B card for your Vigor2136ax.



CSM >> Web Content Filter Profile

Profile Index: 1
Profile Name: Log

Black/White List
 Enable
Action: URL keywords:

Action:

Security

 Bot Nets
 Keyloggers and Monitoring
 Phishing and other Frauds
 Spyware and Adware
 DNS Over HTTPS
 Malware Sites
 Proxy Avoidance and Anonymizers
 Hacking
 Parked Domains
 SPAM URLs

Parental Control

 Abortion
 Alcohol and Tobacco
 Gross
 Low-THC Cannabis Products
 Questionable
 Swimsuits and Intimate Apparel
 Abused Drugs
 Cheating
 Hate and Racism
 Marijuana
 Self Harm
 Violence
 Adult and Pornography
 Cult and Occult
 Illegal
 Nudity
 Sex Education
 Weapons

Productivity

 Auctions
 Dating
 Home and Garden
 Individual Stock Advice and Tools
 Motor Vehicles
 Peer to Peer
 Shareware and Freeware
 Sports
 Web Advertisements
 Computer and Internet Info
 Gambling
 Hunting and Fishing
 Internet Communications
 Music
 Personal Storage
 Shopping
 Streaming Media
 Web Hosting
 Content Delivery Networks
 Games
 Image and Video Search
 Job Search
 Pay to Surf
 Real Estate
 Social Networking
 Training and Tools

General Use

 Business and Economy
 Dynamically Generated Content
 Fashion and Beauty
 Health and Medicine
 Legal
 News and Media
 Philosophy and Political Advocacy
 Religion
 Translation
 Uncategorized Sites
 Computer and Internet Security
 Educational Institutions
 Financial Services
 Internet Portals
 Local Information
 Online Greeting Cards
 Recreation and Hobbies
 Search Engines
 Travel
 Dead sites
 Entertainment and Arts
 Government
 Kids
 Military
 Personal Sites and Blogs
 Reference and Research
 Society
 Web-based Email

Wi-Fi Roaming

Solve the sticky client problem and improve Wi-Fi roaming experience at home when you moving around .

Proactive Roaming

Wi-Fi clients automatically hand-off to another AP/router with a better signal strength when moving around in an area with multiple APs/routers.

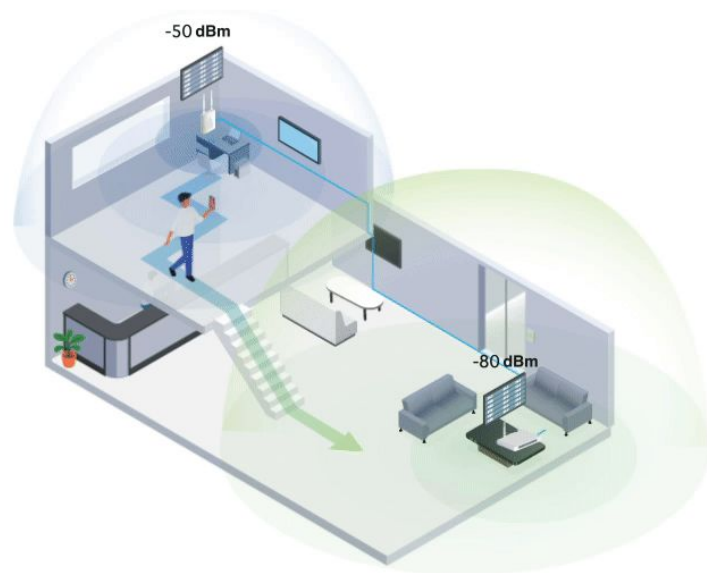
However, Wi-Fi clients sometimes stick to the AP/router with weak signal, and not switching to the one with better signal.

Assisted Roaming

Vigor Router will disassociate the Wi-Fi clients who are out of the effective transmission range, forcing them to pick up another access point/router with a stronger signal.

Stronger Signal Guaranteed

Furthermore, with "Minimum RSSI with Adjacent AP" option, Vigor Router can disassociate the client only when other AP/router has a stronger wireless signal, and keep client stayed when there's no other AP/router nearby.



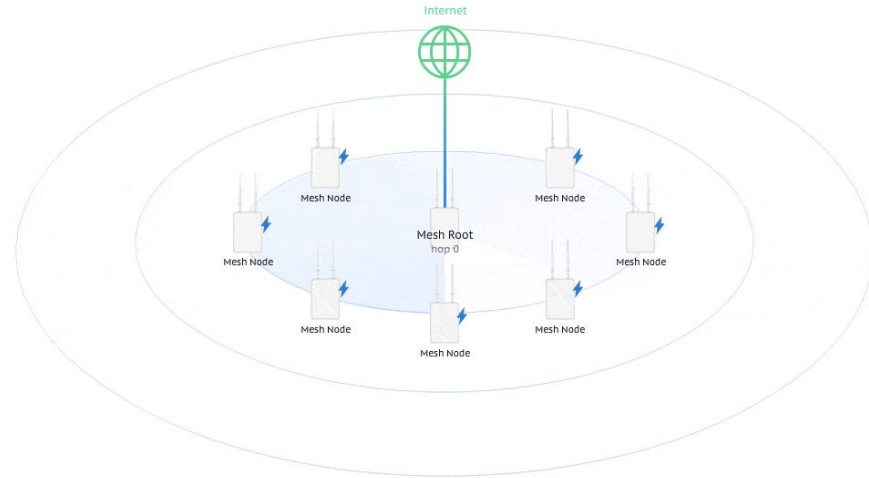
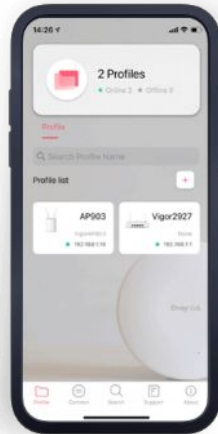
Mesh

From home/SOHO prospect, mesh is more easy. The small hybrid of wired/wireless environment to manage up to 7 APs.

Wirelessly connect 7 APs, and form a Mesh Group
A mesh network creates a set of links automatically and calculate the most optimal wireless path through the wireless network back to a Mesh Root.

Feature:

- Configuration Sync
- Client Roaming
- Client Monitoring with Client List
- Mesh Hierarchy View
- Work with DrayTek Wireless app



Hotspot Web Portal

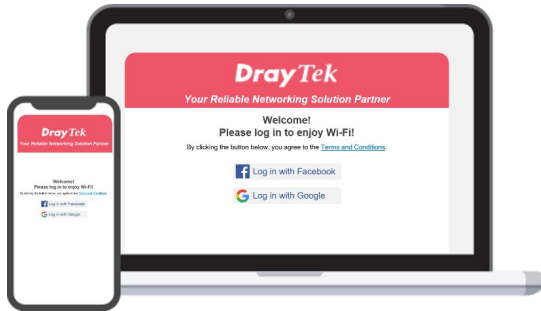
Market your business while offering free Wi-Fi

Wi-Fi Marketing

Redirect the hotspot guests to the company homepage, online surveys, or display promotion message.

Grow Your Email List

Require the guest to leave contact info or social media accounts before they can use the Internet service.



Various Authentication Type

A variety of login methods are supported to meet your business need, including Facebook Login, Google Login, SMS PIN, Voucher PIN, and RADIUS.

3rd-Party Service Compliant

Supports external captive portal authentication. You can keep using the Wi-Fi marketing solution you like.

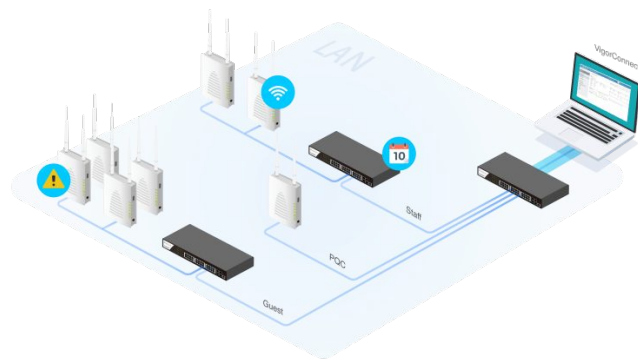
Quota Management

Bandwidth management is integrated into Hotspot to control the bandwidth and session usage of the Hotspot guests.

Designed for Central Management

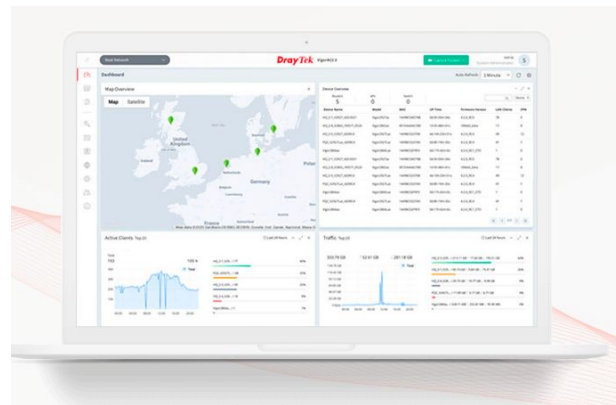
VigorConnect on PC or on Vigor3912S

- Server requirement for PC
Operating System: Windows 7 or later, Linux,
Raspberry Pi 3 B+ or later, Synology NAS (x86 system)
CPU: 1.2GHz Quad Core 64 bits
Memory: 2 GB RAM, Storage: 1 GB
- Vigor3912S (4.3.5.1) support docker. You may install
VigorConnect (1.9.0) to Vigor3912S.



VigorACS (Standalone, Cloud-base)

- Standalone. Please refer the hardware suggestion on
www.draytek.com/products/vigoracs-3/
- Amazon, Google cloud



A white, circular DrayTek access point is shown on a wooden surface. The device has a minimalist design with the 'DrayTek' logo printed in the center. A small triangle and a dot are visible near the bottom edge of the circle. In the background, a blurred green plant is visible against a light-colored wall.

New Products

- DrayOS 5 AP
- VigorAP 1062C
- VigorAP 962C

AP 1062C Product Highlights



Ceiling Mounted AP

Dual Band

4x4, 2.4GHz, 802.11 b/g/n/ax, 1024-QAM

4x4, 5GHz, 802.11 a/n/ac/ax, 4x4 MU-MIMO

AX6000

1148Mbps in 2.4GHz and 4804Mbps in 5GHz

1 x 2.5G LAN

2.5GbE RJ-45

PoE-PD

256 Users

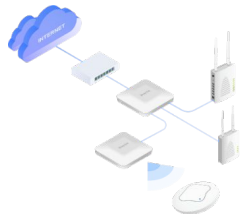
2.4GHz & 5GHz shared concurrently

Key Feature **Central Management**

All-in-One Management

Wireless Virtual Controller

Wireless Nodes: 8 APs
Total Nodes (Wireless + Wired): 50 APs



- Automatically detect Wireless/Wired AP
- AP Discovery
- Auto-Provisioning
- Monitoring

Software Management

VigorACS

*Since ACS 3.5.0
& AP F/W 1.5.2



- Provisioning
- Monitoring
- Centralized Hierarchy View
- Alarm
- Remote AP/Switch/Router Maintenance
- Scheduled Maintenance
- Report

VigorConnect

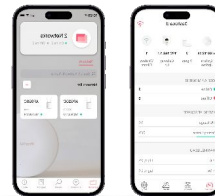
*Since 1.9.0
& AP F/W 1.5.2



- AP/Switch Discovery
- Auto-Provisioning
- Monitoring
- Centralized Hierarchy View
- Alarm
- Remote AP/Switch Maintenance
- Scheduled Maintenance

Wireless APP

*Since 1.3.1
& AP F/W 1.5.2



- Build Wireless Network
- Monitoring
- Parental Control & Client Management
- Mesh Wi-Fi Setup
- Check signal strength and speed test
- Scheduled Maintenance

AP 962C Product Highlights



Ceiling Mounted AP

Dual Band

2x2, 2.4GHz, 802.11 b/g/n/ax, 1024-QAM

2x3, 5GHz, 802.11 a/n/ac/ax, 2x3 MU-MIMO

AX3000

574Mbps in 2.4GHz and 2402Mbps in 5GHz

1 x 2.5G LAN

2.5GbE RJ-45

PoE-PD

256 Users

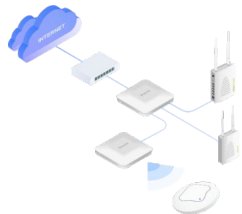
2.4GHz & 5GHz shared concurrently

Key Feature **Central Management**

All-in-One Management

Wireless Virtual Controller

Wireless Nodes: 8 APs
Total Nodes (Wireless + Wired): 50 APs



- Automatically detect Wireless/Wired AP
- AP Discovery
- Auto-Provisioning
- Monitoring

Software Management

VigorACS

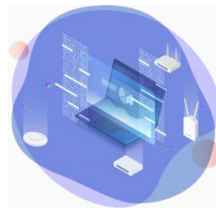
*Since ACS 3.6.0
& AP F/W 1.5.4



- Provisioning
- Monitoring
- Centralized Hierarchy View
- Alarm
- Remote AP/Switch/Router Maintenance
- Scheduled Maintenance
- Report

VigorConnect

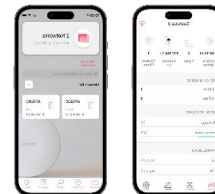
*Since 1.9.2
& AP F/W 1.5.4



- AP/Switch Discovery
- Auto-Provisioning
- Monitoring
- Centralized Hierarchy View
- Alarm
- Remote AP/Switch Maintenance
- Scheduled Maintenance



Wireless APP

*Since 1.3.2
& AP F/W 1.5.4



- Build Wireless Network
- Monitoring
- Parental Control & Client Management
- Mesh Wi-Fi Setup
- Check signal strength and speed test
- Scheduled Maintenance

Vigor Access Point Comparison

	VigorAP 962C 	VigorAP 1062C 
LAN Port	1x 2.5 GbE PoE-In	1x 2.5 GbE PoE-In
Antenna	5 x dual band PiFA internal	4 x dual band PiFA internal
No. of Radio	1 x 2.4GHz + 1 x 5GHz	1 x 2.4GHz + 1 x 5GHz
2.4 GHz Link Speed	574 Mbps	1148 Mbps (4x4)
5 GHz Link Speed	2402 Mbps	4804 Mbps (4x4)
Max. Connective Clients	256 (total radio)	256 (total radio)
Max. Number of SSID	16 (8 per radio)	16 (8 per radio)
2.4 GHz Standard	802.11 b/g/n/ax	802.11 b/g/n/ax
5 GHz Standard	802.11 a/n/ ac Wave 2/ax	802.11 a/n/ ac Wave 2/ax
MIMO	2x3 MU-MIMO	4x4 MU-MIMO

Vigor Access Point Comparison

	VigorAP 962C 	VigorAP 1062C 
Fast Roaming	✓	✓
AP-Assisted Roaming	✓	✓
AirTime Fairness	✓	✓
Band Steering	✓	✓
Managed via VigorAP Mesh Root	✓	✓
Managed via DrayTek Wireless App	✓	✓
Managed via Vigor Router APM	✓	✓
Managed via VigorConnect	Since 1.5.4	Since 1.5.2
Managed via ACS	Since 1.5.4	Since 1.5.2
Suitable Environment	Indoor	Indoor

Mesh – AP Management Compatibility

Root	Node							
	AP 1062C	AP 1060C	AP 962C	AP 960C	AP 906	AP 918R	AP 912C	AP 903
AP 1062C	Y		Y		Y			
AP 1060C		Y		Y		Y	Y	Y
AP 962C	Y		Y		Y			
AP 960C		Y		Y		Y	Y	Y
AP 906					Y			
AP 918R		Y		Y		Y	Y	Y
AP 912C		Y		Y		Y	Y	Y
AP 903		Y		Y		Y	Y	Y

Mesh – AP Management Compatibility

Root	Node							
	AP 1062C	AP 1060C	AP 962C	AP 960C	AP 906	AP 918R	AP 912C	AP 903
2136ax	Y		Y					
2135ac/2765ac/2766ac		Y		Y		Y	Y	Y
2135ax/2765ax/ 2766ax	Y		TBD		Y			
2927ac/2865ac/2866ac		Y		Y		Y	Y	Y
2927ax/2865ax/2866ax	Y		TBD		Y			
2862ac/2926ac								Y
2763ac		Y		Y		Y	Y	Y

Wireless Virtual Controller

Intelligent Auto-Configuration

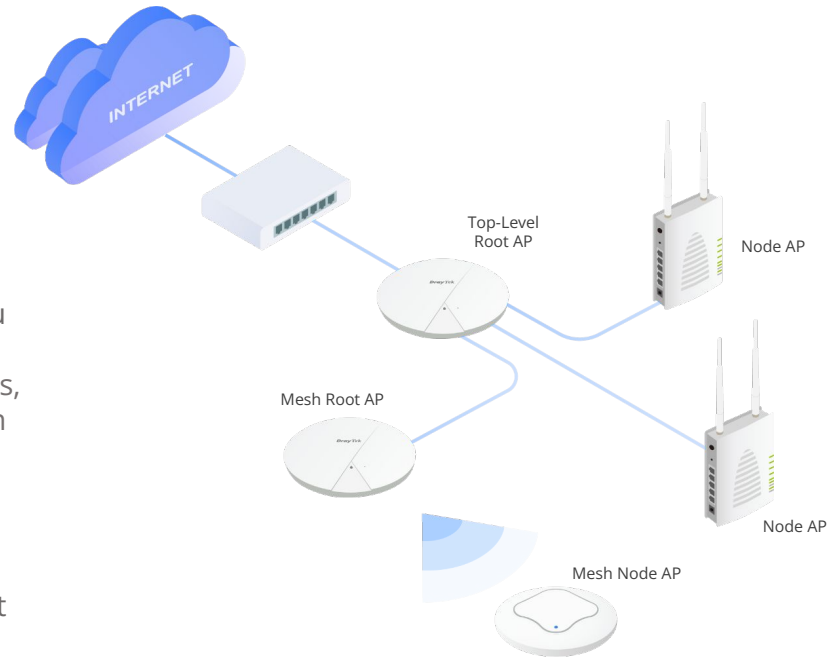
Once connecting to AP1062C, this feature can detect the type of AP, wired or wireless, and automatically determine the most appropriate network topology. For smaller wireless environment with fewer than 8 APs, it seamlessly enables Mesh mode; while in larger wired installation with more than 8 APs, then AP management mode will be activated for enhanced control and scalability.

Wireless Device Monitoring

The panel provides a comprehensive view of your network, allowing you to easily monitor devices, mesh status, and nearby APs. With the ability to monitor AP devices, it enables to check WLAN clients, MAC, IP address, Status, SSID of each radio, number of clients, and firmware version all in one page, even AP offline can be spotted. It is much more easier to manage and optimize network with ease effectively.

Zero Touch Deployment

After auto-detecting and adding Node AP into management group, Root AP will provision the relevant AP configurations to node APs.



Wi-Fi Roaming

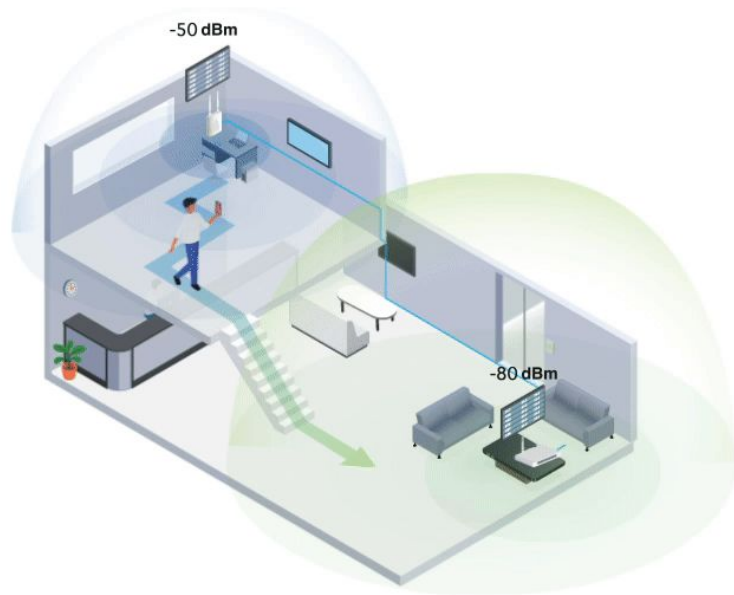
Solve the sticky client problem and improve Wi-Fi roaming experience.

Roaming Protocol

VigorAP 1062C supports 802.11r and 802.11k roaming protocols. These protocols enable Wi-Fi clients to seamlessly transition to another AP/router that offers a stronger signal when moving within an area that has multiple APs/routers. Clients that are also compatible with these roaming protocols will experience the advantages of proactive roaming.

Assisted Roaming

The "Minimum RSSI with Adjacent AP" option in VigorAP allows for the dissociation of a client only if there is another adjacent AP/router that provides a stronger wireless signal to the client. Otherwise, the client will remain connected.



What's New on **DrayOS5 AP**

Enhanced user-friendly configuration design for wireless LAN

Compared to DrayOS4, where SSID, Radio Settings, Roaming and other wireless setup info need to be configured on different pages. Starting from DrayOS5, these settings can be conveniently completed in the same page under Configuration >> Wireless LAN, providing an easier and more clear wireless configuration experience.

Notification Service

DrayOS5 APs can send notifications to the DrayTek Wireless App when detecting client disconnections, mesh node offline, and login events. The network admin can conveniently receive notifications for wireless network events from his phone.

MAC Filtering for Access Control List

This feature helps prevent unauthorized devices from connecting to AP. To enable Access Control and set up Allow/Block policy in DrayOS5, go to Security >> MAC Filtering Profile to generate profile list by adding Name and MAC address, then turn to Configuration >> Wireless LAN, apply the MAC Filtering List into SSID Settings to complete Access Control management.

What's New on DrayOS5 AP

View Clients wireless status in one page

In DrayOS4, client related info is presented separately in Wireless LAN 2.4GHz or Wireless LAN 5GHz. From now on, you can check both channel clients in Monitoring >> Clients List, which shows more details to help you comprehensively manage client information in a single page.

Clients List

 Refresh

MAC	Up Time	Link Speed	RSSI	SSID	Usage Up	Usage Down	CH	Band	BW	Physical Mode	Auth Mode	Encrypt Type
	0d 03:00:11	432 Mbps / 6 Mbps	26% (-79dbm)	guests_4F	18.258MB	3.583GB	36	5GHz	80M/80M	802.11ax	WPA3 Personal (FT)	AES
	0d 02:47:25	585 Mbps / 702 Mbps	60% (-66dbm)	staffs_4F	56.611MB	96.057MB	36	5GHz	80M/80M	802.11ac	WPA2 Personal	AES
	0d 02:41:22	585 Mbps / 24 Mbps	34% (-76dbm)	staffs_4F	82.659MB	39.246MB	36	5GHz	80M/20M	802.11ac	WPA2 Personal	AES
	0d 02:25:18	433 Mbps / 24 Mbps	60% (-66dbm)	staffs_4F	8.030MB	14.929MB	36	5GHz	80M/80M	802.11ac	WPA3 Personal (FT)	AES
	0d 00:20:18	960 Mbps / 24 Mbps	42% (-73dbm)	staffs_4F	828.744KB	3.000MB	36	5GHz	80M/20M	802.11ax	WPA3 Personal (FT)	AES
	0d 00:36:48	720 Mbps / 24 Mbps	39% (-74dbm)	guests_4F	2.724MB	4.698MB	36	5GHz	80M/80M	802.11ax	WPA3 Personal (FT)	AES
	0d 00:19:32	72 Mbps / 65 Mbps	81% (-58dbm)	guests_4F	21.151MB	8.350MB	1	2.4GHz	20M/20M	802.11n	WPA2 Personal	AES



AP805



Desk Stand AP

Dual Band

2x2, 2.4GHz, 802.11 b/g/n/ax, 1024-QAM
2x3, 5GHz, 802.11 a/n/ac/ax, 2x3 MU-MIMO

AX3000

574Mbps in 2.4GHz and 2402Mbps in 5GHz

2 x LAN

1 x 2.5GbE RJ-45
1 x 1GbE RJ-45

256 Users

2.4GHz & 5GHz shared concurrently

