

# What's New in Fireware v12.0.2

# What's New in Fireware v12.0.2

- Wireless Firebox Enhancements
  - KRACK WPA/WPA2 client vulnerability mitigation





# Fireware Wireless Enhancements

# KRACK WPA/WPA2 Vulnerability Mitigation

- Access point WPA/WPA2 key reinstallation vulnerabilities were addressed in Fireware v12.0.1 for wireless XTM devices and wireless Fireboxes:
  - XTM 25-W, 26-W, 33W
  - Firebox T10-W, T15-W, T30-W, T35-W, T50-W, T55-W
- Client vulnerabilities must be addressed on each client
- Until all clients are patched, you can mitigate client WPA/WPA2 vulnerabilities with wireless Fireboxes
- Client mitigation blocks handshake messages that can potentially exploit clients and forces clients to reauthenticate

# KRACK WPA/WPA2 Vulnerability Mitigation

- Configured in **Network > Wireless**
- Disabled by default
- The mitigation logic can trigger for similar dropped packet symptoms, for example, natural frame errors during a handshake, or dropped packets when a client roams
- Can result in some client connections to fail and be reestablished
- We recommend that you enable this option until all clients are patched

Enable wireless access points

Access point 1 Enabled [CONFIGURE](#)

Access point 2 Disabled [CONFIGURE](#)

Access point 3 Disabled [CONFIGURE](#)

Radio Settings

The WatchGuard XTM Wireless is intended for indoor use only

Country of Operation

Frequency Band  2.4GHz  5GHz

Wireless Mode  ▾

Channel  ▾

Channel Width  ▾

Extension Channel  ▾

Transmit Power  ▾

Fragmentation Threshold  bytes

RTS Threshold  bytes

Enable WPA/WPA2 vulnerability mitigation

Enable rogue access point detection [CONFIGURE](#)



**Thank You!**

***NOTHING GETS  
PAST RED.***



**WatchGuard Training**

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved