Secure Network Solutions from ECRS

Routers, Access Points & Security Services
Supporting Security and Compliance

August 2018

Authors

Jesse Dyer, QIR
Vice President of Support

Matthew Mellon, CISSP, QIR
Chief Information Security Officer

Contents

EXECUTIVE SUMMARY

The network equipment used by a merchant is the foundation of reliable retail operations. Routers and wireless access points must be secure, durable, affordable, and and able to facilitate the regulatory requirements applicable to your particular business model. Merchants with different business models have different needs.

In 2011, ECRS began producing routers that revolutionized the status quo for merchant networking equipment. We started with the venerable ASUS RT-N16 router and added highly customized firmware to help merchants achieve compliance, security, and reliable Wi-Fi connectivity. Key features included operating on the 2.4 GHz band at legal limit power, TLS-based site-to-site VPN, and strong Wi-Fi security defaults – all at affordable prices.

The ASUS RT-N16-based routers sold by ECRS since 2011 are reaching end of sale life on July 1, 2018. This is due in large part to the reduced availability of components in the router.

ECRS stands ready with new top-notch durable network appliance offerings which will make your networks more secure and easier to manage.

ECRS stands ready with new top-notch durable network appliance offerings which will make your networks more secure and easier to manage. These new product offerings were selected with interoperability and adaptability in mind. WatchGuard Firebox brand next generation routers form the core of our new line of network appliances.

Factors Driving Choice of Equipment

Longevity, Obsolescence, and Updates

With your network forming the foundation of a reliable point of sale system, you need devices that have low failure rates and are backed by the manufacturer and reseller for the life of your investment.

The WatchGuard Firebox lineage of network security appliances has an excellent track record for device longevity. Standard WatchGuard support availability extends for 5 years past end-of-sale for each model.[1]

Watchguard continually improves Fireware, the Firebox operating system, and firmware upgrades are simplified to just a few clicks, making it easy for you to stay ahead of emerging threats.

Cloud Readiness

Each physical location in your retail enterprise needs an an edge router to connect it to the Internet. The WatchGuard Firebox can also run as an appliance in your store's private cloud. There are advantages to running the hub of your hub-and-spoke VPN in the cloud:

- Private clouds offer extremely good network speeds and low latencies with regionally located data centers and fault-tolerant hardware deployments.
- Using the cloud, you can centralize subscription security services like WebBlocker and Data Loss Prevention without being constrained by the bandwidth at your physical central office.
- When something goes wrong in the cloud, problems can be corrected within minutes. Physical RMA processes typically involve next-day replacements.

VPN Interoperability

For any merchant with more than one location, VPN is key to interconnecting your locations securely. Many merchants have heavy investments in existing site-to-site and site-to-cloud VPN termination equipment, including OpenVPN protocol based digital® VPN Concentrator (DVPNC) devices, traditional IPSec-capable routers, and ASUS routers with digital® firmware. You must select compatible equipment for new sites to avoid a costly rip-and-replace transition.

WatchGuard Firebox routers from ECRS are wholly compatible with existing DVPNC/ASUS site-to-site and site-to cloud deployments, and are capable of operating both OpenVPN tunnels and IPSec tunnels simultaneously, so you can extend and replace your network infrastructure at your own pace.

[1] Watchguard. (2018, June 25). *End of Life Policy*. Retrieved from https://www.watchguard.com/wgrd-resource-center/end-of-life-policy .

Wi-Fi Band Selection

Merchants today face challenging Wi-Fi environments due to the proliferation of connected devices on the 2.4 GHz (microwave) band. Depending on the model selected, WatchGuard Firebox brand wireless routers support either a choice of 2.4 GHz and 5 GHz bands, or are capable of operating both simultaneously. All supported Catapult HHT terminals support both bands. WatchGuard devices give you the flexibility you need to conquer Wi-Fi problems.

Network Segmentation

Many need to segment their networks to allow secure guest wireless access or to reduce their PCI validation scope.

WatchGuard devices give you the flexibility you need to conquer Wi-Fi problems.

PCI DSS Compliance and Validation

Your payment card processing solution determines the applicability of PCI DSS requirements to your network equipment. The payment card acquirer ultimately approves or denies any scope reductions.

- If you are a merchant processing branded payments exclusively via the ECRS Direct Connection to First Data Rapid Connect using approved end-to-end encrypted payment card readers, First Data (your acquirer) will grant you a scope reduction allowing you to exclude your network equipment from validation scope.
- If you are a merchant processing branded payments exclusively via WorldPay using point-to-point encrypting card readers, then WorldPay may grant you a scope reduction under certain circumstances.
- If you outsource your payment processing to USA Technologies and use only point-to-point encrypting payment card readers approved by USA Technologies, USA Technologies does not require you to complete annual validation.
- If you use traditional payment processing using non-encrypting payment card readers, your network equipment is fully in-scope for validation.

Regardless of the validation requirements, you should understand that the security of your network equipment remains important to minimize risk of non-payment card related data breaches and operational risk (potential downtime).

Depending on your validation and risk mitigation requirements, ECRS will recommend different solutions to meet your business needs.

WatchGuard Firebox and AP Devices: Addressing Emerging Requirements

In 2011, ECRS began producing routers that revolutionized the status quo for merchant networking equipment. We started with the venerable ASUS RT-N16 router and added highly customized firmware to help merchants achieve compliance, security, and reliable Wi-Fi connectivity. Key features included operating on the 2.4 GHz band at legal limit power, TLS-based site-to-site VPN, and strong Wi-Fi security defaults – all at affordable prices.

Fast-forward to 2018, and the landscape has changed. Key improvements in network technology have emerged:

- **Wi-Fi devices from major manufactures now support the 5 GHz band in addition to the legacy 2.4 GHz band.**
    - 5 GHz offers faster speeds at shorter distances.
    - 5 GHz devices are less likely to be impacted from environmental interference.
    - Far more channels are available in the 5 GHz band than in the 2.4 GHz band.
    - 5 GHz availability is an important tool for merchants to have in a challenging 2.4 GHz environment.
- **Router-based firewalls are much "smarter" now than ever.**
    - Legacy router-based firewalls like the RT-N16 employ a technique called "stateful packet inspection" or SPI, which the decision about whether to allow or deny each packet based on source and destination address and port, and whether each packet is part of an "existing" connection.
    - Next-generation router-based firewalls provide deeper, stronger security by also operating at the application layer. These routers also examine the payload of each packet. It's a bit like opening up a truck and looking at the cargo rather than just checking a license plate. This allows allowing and disallowing traffic based on application or category of content.
    - Some next-generation router-based firewalls can also perform data loss prevention. For example, a router can open up every egressing packet and verify that it contains no unencrypted credit card numbers.
- **Frequently emerging threats mean you need a router that can be easily updated.**
    - In recent years, major vulnerabilities in TLS encryption libraries and in the Linux kernel necessitated many security releases from router vendors across the industry.
    - Merchants don't have the time or often the expertise to monitor for these emerging threats or to perform cumbersome and risky upgrades on their own networking equipment.
    - You need equipment that seamlessly obtains and installs updates from the cloud, without lengthy or difficult upgrade procedures.

Hardware Recommendations

Multi-Store Enterprise

Transitioning from ASUS/DVPNC to WatchGuard Firebox

As long as any remote store exists using an ASUS RT-N16 with digital™ firmware, the merchant must also have a digital™ VPN Concentrator or a digital™ VPN Concentrator cloud instance.

Enterprises with an on-premise digital™ VPN Concentrator must transition to a digital™ VPN Concentrator cloud instance when implementing Firebox Cloud. On-premise OpenVPN Access Server licenses are portable to digital™ VPN Concentrator cloud instances.

WatchGuard Firebox units can also be added as new or replacement remote store edge routers while an enterprise continues to use a digital™ VPN Concentrator.

Multi-factor Client VPN Access Requires digital™ VPN Concentrator

At this time, a digital™ VPN Concentrator is also still required if your business needs client-to-site VPN with multi-factor authentication (e.g. a work-at-home employee, tablet-based POS over LTE, or Catapult HHT over LTE on iPhone).

ECRS recommends that each multi-store enterprise have a Watchguard Firebox Cloud instance, establish VPN tunnels between that cloud datacenter and each business location, and route all traffic through the cloud. This topology is advantageous because:

- By routing all traffic through a single Firebox instance, you can purchase subscription security services covering all traffic at a much lower cost.
- By routing all traffic through a cloud datacenter, you can avoid a single physical location being a bandwidth bottleneck.

Model Size Guidelines for Firebox Cloud instances

Number of remote stores and warehouses	Size of Firebox Cloud instance
50 or fewer	Small
51 to 600	Medium
601 to 6000	Large

Alternatively, ECRS will support a cloudless topology for a multi-store enterprise with all traffic routed through a single physical location. This may work well for a multi-store with few remote stores and/or high bandwidth at the HQ location (e.g. gigabit Internet service). However, it may be necessary to move the hub of the topology to the cloud if bandwidth is insufficient. Common high bandwidth consumption activities include backups of large databases, automatic software updates, and streaming video (e.g. security cameras).

Single and Remote Stores

Routers

Each single store or remote store/warehouse requires a WatchGuard Firebox.

Model Sizing Guidelines for Firebox units

Store Size	Model
Unattended micro-market kiosk or very small store (<1200 ft^2)	Firebox T15-W
Traditional brick-and-mortar store or warehouse	Firebox T35 (wireless access point also needed)

Wireless Access Points

Wireless access points are required for merchants wishing to take advantage of CATAPULT HHT, to connect computers or AutoScale units wirelessly, or to offer guests access to the Internet. Consumer-grade wireless equipment is insufficient to meet modern security requirements for a retail environment.

About 2.4 GHz and 5 GHz Wireless Network Bands

All CATAPULT HHT terminals sold by ECRS since 2015 support both bands; however, some older laptops and many cellular telephones do not support 5 GHz wireless. 5 GHz band coverage is important in many challenging wireless environments.

- For very small stores (<1200 ft^2) and micro-market kiosks, the WatchGuard Firebox T15-W is sufficient. **The Firebox T15W is capable of providing wireless coverage for a small store (<1200 ft^2) on either the 2.4 Ghz or 5 GHz band, but not both at the same time.**
- ECRS recommends WatchGuard AP320 wireless access points for all other stores. The AP320 is capable of providing secure access on both 2.4 and 5 GHz bands simultanouesly.
- If you are replacing an ASUS RT-N16 wireless router with a WatchGuard Firebox T35, you will also need to purchase a WatchGuard AP320 to retain wireless capabilities.
- As a rule of thumb, one AP320 is required per 1500 ft^2 of coverage area. However, additional access points may be required depending on your particular wireless environment.
- Up to one AP320 can be powered directly off of the Firebox T35 using the included PoE port. Additional units will require either a PoE switch or a power supply. ECRS offers Allied Telesis brand switches.

Security Service Recommendations

Security features on WatchGuard Firebox are available on a subscription basis. For details about the available security features, see https://www.watchguard.com/wgrd-products/security-services.

Routers

ECRS recommends different security service packages depending on your PCI validation requirements and other risk factors.

Your payment processing acquirer determines whether or not your network is in-scope for PCI DSS compliance validation. ECRS strongly recommends exclusively using a processing solution with P2PE or E2EE encryption that removes the point of sale terminals and their network from validation scope.

Consider all risks

Payment card data breaches are not the only risk to your business. Merchants may also store personally identifiable information (PII), HIPAA protected health information (PHI), and other types of sensitive data. Malicious attackers also pose other operational risk to your business. Even data isn't stolen, if an attacker shuts down your business with ransomware or another attack, you won't be able to serve your customers.

If your networks are completely out of scope for PCI DSS validation, you may eschew all subscription security services, but this is not recommended. Even with the reduced validation requirements, ECRS still recommends, at minimum, WatchGuard Basic Security Suite. For the best protection, purchase WatchGuard Total Security Suite. Only you can accept risk on behalf of your business.

Security Service Recommendations by Store Size

Risk Scenario	Recommendation
Single store with in-scope network	WatchGuard Total Security Suite
Single store with out-of-scope network	WatchGuard Basic Security Suite
Enterprise with in-scope network	WatchGuard Total Security Suite at Firebox Cloud only. **VPN must not split-tunnel.**
Enterprise with out-of-scope network (e.g. with First Data TransArmor Data Protection)	WatchGuard Basic Security Suite at Firebox Cloud only. **VPN must not split-tunnel.**
Micro-market kiosk merchant with legacy payment processing	No subscriptions at stores or central office, Watchguard Total Security Suite at Firebox Cloud. **VPN must not split-tunnel.**
Micro-market kiosk merchant with USA Technologies payment processing	No subscriptions at stores or central office, Watchguard Basic Security Suite at Firebox Cloud. **VPN must not split-tunnel.**

By using policies to route all multi-store traffic through a Firebox Cloud, security services can be applied centrally, saving on subscription costs for individual stores.

Wireless Access Points

Three tiers of subscriptions are available for WatchGuard access points: Total Wi-Fi, Secure Wi-Fi, and Basic Wi-Fi.

- Merchants wishing to provide guest wireless access with a captive login portal must also purchase a WatchGuard Total Wi-Fi subscription.
- WatchGuard access points are capable of using a mesh network topology to allow some access points within a store to operate without a wired connection. To take advantage of this feature, a WatchGuard Secure Wi-Fi or Total Wi-Fi subscription is required.
- For all other merchants, ECRS recommends a WatchGuard Basic Wi-Fi subscription.

Legal Notice

The information in this document is related specifically to the operations of merchants in the United States. Additional requirements may alter the applicability of information in this document to a particular merchant in a particular jurisdiction.

The content of this document is provided for informational purposes only, and is not intended to and should not be relied upon or construed as a legal opinion or legal advice regarding any specific regulatory issue or factual circumstance. The document is provided without any representation or warranty whatsoever regarding the accuracy or completeness of the information. Any specific questions about PCI DSS compliance validation should be addressed to your payment card acquirer.

Content Update Change Log

Date	Change

About ECRS

ECRS is an industry-leading retail solutions provider harnessing technology to future-proof today's retailers and prepare them for tomorrow's opportunities. ECRS' revolutionary CATAPULT® system is the market's only truly unified point of sale platform. With CATAPULT, the point of sale, self checkout, web-store, inventory, customer loyalty, back office, e-commerce, and enterprise management all share a single transactional business logic. We call this Unified Transaction Logic™, empowering our retailers to prosper by providing actionable business intelligence across the enterprise. Unifying hardware, software, and services, ECRS offers a friction-free, cost-saving solution that will increase customer engagement and improve the consumer experience.

ECRS is committed to perpetual development, expanding value through constant innovation. To that end, CATAPULT is fully-customizable. Optional plug-and-play modules work seamlessly with core applications, offering retailers freedom and flexibility in designing their point of sale platform. Retailers can easily expand platform functionality as their business grows. Exhaustive research, intelligent design, and rigorous pre-market testing ensure that ECRS products integrate smoothly into existing retail environments.

ECRS' technology solutions are backed by a knowledgeable, accessible, and award-winning US-based support team that is dedicated to retail success. On the 2017 RIS Leaderboard, ECRS was ranked #1 for grocery vendors for the fifth year in a row, #1 for midsize retailers, and ranked in the top 5 for quality of support for the ninth year in a row.

ECRS is proud to be building a community of retailers and share in their success.

Systems that ECRS Innovates

Traditional Point of Sale
Self-Checkout Systems
Click & Collect 2.0
Mobile POS
Accelerated Checkout®
Back Office Management
Reporting & Analytics
Customer Loyalty & Marketing
Enterprise Headquarters Management
Inventory & Warehouse Management
Supplier & EDI Integration
Gift Card Systems
Membership Management
Fuel Pump Integration
Pharmacy System Integration
Onboarding & Support Services

800.211.1172
solutions@ecrs.com
www.ecrs.com
www.ecrs.com/linkedin
www.ecrs.com/twitter
www.ecrs.com/youtube
www.ecrs.com/facebook
www.ecrs.com/gplus