NATting Else Matters: Evaluating IPv6 Access Control Policies in Residential Networks

Karl Olson, Jack Wampler, Fan Shen, and Nolen Scaife

University of Colorado Boulder
{karl.olson,jack.wampler,fan.shen,scaife}@colorado.edu

Abstract. Customer edge routers are the primary mode of connection to the Internet for a large portion of non-commercial users. As these consumer networks migrate from IPv4 to IPv6, stateful firewalls are needed to protect devices in the home. However, policy details crucial to the implementation of these inbound access controls are left to the discretion of the device manufacturers. In this paper, we survey ten customer edge routers to evaluate how manufacturers implement firewalls and user controls in IPv6. The result is a systemic, demonstrable failure among all parties to agree upon, implement, and communicate consistent security policies. We conclude with future research directions and recommendations for all parties to address these systemic failures and provide a consistent model for home security.

Keywords: IPv6 · Consumer Gateway · Network Address Translation · Security.

1 Introduction

For over twenty years, IPv4 network address translation (NAT) dictated a common operational template for customer edge (CE) routers across a diverse set of hardware manufacturers. Fueled by Internet growth and address scarcity rather than intended design, the ubiquitous usage of NAT, combined with RFC 1918 addressing, provides consumers and developers with a common behavioral standard [21,20]. While unintentional, NAT meaningfully isolates devices inside the network from those outside it. This allows device manufacturers, and consumers by proxy, to benefit from automatic and default attack surface reduction.

In contrast, IPv6 provides enough address space that individual devices receive their own public, globally-routable addresses. This model eliminates the need for NAT and allows other devices on the Internet to communicate directly with devices in the home. The IETF provides little guidance or standard for firewall configurations [16,3], allowing router manufacturers to implement filtering policies at their own discretion. With approximately two-thirds of consumer devices maintaining default settings [6] or failing to keep up with system or security updates [17], internal devices' exposure to external threats becomes dependent on the router's design. Without a default security perimeter in place, once "secured" devices within a home network now rely on the consumer to either individually maintain each device or to implement a technical solution, such as detailed firewall rules, on their own.

In this work, we perform the first study of IPv6 CE routers to examine how manufacturers are implementing filtering and access control for IPv6 residential networks. We assess ten popular CE routers to evaluate their default firewall policies and the ability for consumers to implement custom rules. Our findings show inconsistency in the implementation of default configurations, overexposure of services, and an overall lack of messaging to consumers about the baseline policy of a device. As a result, in cases where no default firewall is enabled, consumers may be unaware of the exposure of their devices and developers may have incorrectly assumed that a device's services are not exposed to the Internet.

The remainder of this paper is structured as follows: In Section 2, we provide a short overview of IPv6 features, operation considerations and competing security paradigms. We then present our methodology for assessing IPv6 implementation in CE routers across a spectrum of features and configurations in Section 3 before presenting our results in Section 4. We discuss the necessity for a single device baseline standard and recommend consistent messaging in Section 5. Finally, we conclude in Section 6.

2 Background

Although functionally similar to IPv4, IPv6 provides a few small but impactful changes to the typical consumer network. In this section, we give a brief history of the transition from IPv4 to IPv6 before covering some key differences between the two protocols and their potential impact on consumers.

2.1 IPv4 NAT

NAT shaped the CE routing environment for two primary reasons: First, the scalability of NAT delayed the eventual address exhaustion of IPv4 in a period of explosive Internet growth and provided a simple path to connect significantly more devices to the Internet. Internet Service Providers (ISPs), who manage public address distribution in their networks, effectively required CE routers to support NAT by allocating exactly one public IP to each household gateway [8].

Second, the simplicity of NAT lowered the barrier for non-technical users to operate their own network. Home networks are often unmanaged or rely heavily on default configurations to meet the needs of non-technical users [3,20,4]. By adopting NAT, CE routers were able to provide simple or automatic initialization that required minimal configuration beyond Service Set Identifier (SSID), Wi-Fi Protected Access (WPA) password, and any ISP-specific settings (such as a PPPoE username/password) [4]. Once established, a suite of protocols (UPnP, STUN, etc.) provide an interface for connected devices to negotiate with the router directly such that the user would rarely need to interact with the network [7,19,16]. NAT also removed the need to define and manage an ingress filtering policy, as the one public address is multiplexed for use by all internal hosts. The prevalence and ubiquity of NAT are now synonymous with the default-deny ingress policy that has become the de facto security model of CE networks, a policy that *is often the only ingress access control deployed.*

However, the motivation for the adoption of NAT in IPv4 is negated by a core feature in the design of IPv6: there is no longer an addressing shortage meaning we again have the ability to assign one or more addresses to each device. With this transition, inbound access controls are now discretionary; IPv6 allows CE networks to operate without the network perimeters and default access control necessitated by NAT.

While the IETF explicitly acknowledges that care should be taken in designing the baseline operation of CE routers, they avoid proposing default configurations due to a constructive tension between the desires for transparent end-to-end connectivity on the one hand, and the need to detect and prevent intrusion by unauthorized public Internet users on the other [20]. The strongest recommendation provided by the IETF is for manufactures to include a toggle to allow customers to choose between an open, unfiltered gateway where security is left to endpoint devices, or a closed perimeter approach, similar to NAT, where traffic is filtered and only allowed through careful exception [3,20]. In the absence of efforts by manufacturers to provide standardization or documentation of the defaults that they implement, consumers are left to assess whether the security model that their network implements is sufficient.

2.2 IPv6 Reachability

A significant consideration in the adoption of IPv6 is the ability to uniquely address each device that joins the Internet. No longer defined by NAT architectures and private subnets, this addressing allows for every device to be globally *reachable*. Devices designed for the home environment often pose a serious risk when exposed to the open Internet [10,9,2]. However, globally reachable does not automatically imply a device is globally *accessible*.

The IETF's RFCs give router manufacturers discretion for handling unsolicited inbound traffic in IPv6. The two basic options for default policies are:

- **Default Deny**: drop all unsolicited WAN-to-LAN inbound traffic. To permit inbound traffic, users can either manually add firewall exceptions or rely on protocols that allow exceptions to be negotiated directly with the router. This policy resembles the existing model of IPv4 networks instrumented with NAT and UPnP.
- **Default Permit**: allow unsolicited inbound WAN-to-LAN traffic. Devices are globally accessible, offloading the responsibility for filtering unwanted traffic to each individual device. The advantage of this model is that developers can easily design and deploy their Internet-capable devices without consideration for including and maintaining additional security mechanisms such as firewalls, hole punching mechanisms, or their associated user interface controls.

Whichever default policy is used, the mental model that a user employs must change from that of IPv4. If a user wishes to manually configure an exception to the ingress policy that their router implements, the subtle difference between NAT and individually globally-addressed devices is significant. For example, individual devices in IPv6 can have more than one address assigned concurrently, and those addresses may be link-local or transient as demonstrated in Figure 1. In order to administer their IPv6 network in a manner equivalent to IPv4, users must understand technical details about IPv6 operation and firewall behavior. This is further complicated by the fact that the control interfaces provided by manufacturers and across devices have no

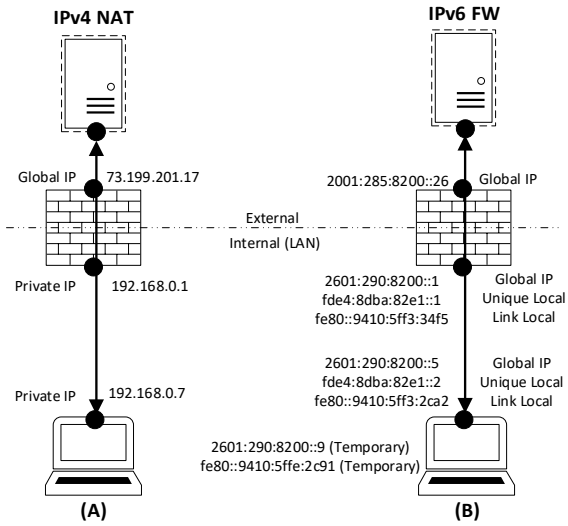

Fig. 1: **IPv6 Network Layout** – IPv6 represents a fundamental shift in the addressing of local networks. In (A) NAT, computers follow a one-to-one mapping of local network private IP with a single globally-routable IP shared by many internal devices. In (B) IPv6, devices can have many addresses depending on operational scope. Additionally, IP addresses are unique and can be routed globally if it has the correct scope – a direct contrast to IPv4 NAT.

common nomenclature or abstractions for configuration tasks. A study of enterprise IPv6 networks found that enterprise operators likewise have difficulty implementing appropriate controls in these networks [5]. These challenges should not imply that there is anything inherently wrong with IPv6 - the same model provided by IPv4 NAT can similarly be implemented in IPv6 [18] - but further demonstrate the need to provide a common expectation for baseline operation.

The flexibility of implementation among CE routing devices combined with globally reachable addressing creates a potential issue: unlike IPv4 networks where the de facto model is effectively required, in IPv6 CE routers are free to expose all internal endpoints. Furthermore, as devices transition from IPv4 to IPv6, this exposure could occur without any communication to the end user as they attempt to administrate their network. Because inbound access control implementation is left to the discretion of manufacturers, we suspect that there is variance among implementations. In the next section, we describe our methodology for evaluating a set of off-the-shelf CE routers to assess how IPv6 access control is implemented in practice.

3 Methodology

Our study aims to measure the security implementation of consumer grade gateways and the configuration options that they provide for IPv6. In this section, we describe our methodology for selecting and evaluating these routers.

3.1 Router Selection and Network Configuration

In order to choose routers that are representative of those deployed in real networks, we rely on the work of Kumar *et al.*, who provide insight into the most commonly used global gateways by manufacturer and region [10]. Out of 4.8K router vendors globally, we selected 12 routers which covered 25.2% of the most commonly deployed global brands. Only routers that specifically mention compatibility with IPv6 were chosen for our comparison. We were unable to find any routers that advertise or provide messaging about filtering policies. To evaluate the potential differences within a manufacturer we include multiple Linksys (`EA3500`, and `EA6350`) routers. Two of the selected routers (the `Tenda AC18` and the `Wavlink Aerial G2`) were excluded because they did not actually support IPv6 upon arrival. The remaining ten devices used in our assessment are shown in Section 4, Table 1.

Our architecture consists of four key elements marked with letters in Figure 2. Two vantages were established to assess traffic flows: an external host located on a public cloud provider (A) scanning across a public ISP toward the firewall (B) or internal host (C), and an internal vantage (D) which conducted the same scans focused outbound (with the exception of targeting an external host due to the ubiquitous outbound permit policy of the firewalls). All devices sending and receiving probes associated with scans were under our control at all times and at no time did we perform any scanning or analysis of public or private systems outside of our controlled scope. This architecture allowed us to pass traffic across the public internet via local consumer grade ISPs and through the assessed routers from different vantages to analyze real-world operational modes.

3.2 Evaluation Methodology

In order to allow unsolicited inbound connections (e.g., peer-to-peer connections), IPv4 routers must provide the ability to *port forward*; the router establishes a list of port numbers and destination (internal) addresses. When a packet is received on the public interface at a port in the list, the router bypasses any NAT lookup and immediately rewrites the destination address and forwards the packet internally. Forwarding is common in IPv4; devices rely on the UPnP and NAT-PMP protocols to automate the setup of forwarding rules. Without these protocols, users would need to manually create such rules, a technical task requiring knowledge of IP addresses and TCP/UDP ports.

Forwarding is effectively meaningless in IPv6 without NAT as devices can be addressed directly. Instead, routers must provide a mechanism to create firewall exceptions if a firewall is implemented. While these rules can be as simple as port forwarding rules (e.g., a destination IP and a port number), how they are implemented and the options available to users may vary. We evaluate the following basic characteristics of each router:

- **Default IPv6.** We first check if each router supports IPv6 and whether it enables that support by default. When IPv6 is enabled by default, IPv6-capable devices on the internal network automatically request addresses. Default IPv6 support requires that the upstream ISP also supports IPv6. It is notable that router support for IPv6 and default enable state can be changed in a firmware update

pushed remotely by the manufacturer, and ISPs can (and do) add support for IPv6 without notifying consumers. Therefore, *devices in the home environment can transition to IPv6 overnight without the user's knowledge.*

- **Firewall Present.** Next, we evaluate whether or not the device implements a firewall. In cases where a firewall is not present, the device will pass all traffic to internal hosts.
- **Firewall Enabled.** If a firewall is present, we evaluate whether or not it is enabled (i.e., filtering) by default.
- **One-Click Open.** While RFC 7084 refrains from proposing a default IPv6 ingress filter policy for consumer gateways, it advises that gateways implement a single button to toggle all firewall ingress filtering [16]. We evaluate whether or not the device includes this functionality.
- **Security Warning.** When the One-Click Open option is used, we evaluate if there is any warning or communication to the user about the danger of disabling the firewall.
- **Rule Generation.** We evaluate whether each device includes the ability to create exceptions to the default firewall policy. Such rules may be necessary for allowing specific services or applications to function in the presence of a firewall. Because we are comparing to existing functionality in IPv4 networks, we specifically exclude examining more expressive firewall capabilities than IP/device/port tuples.
- **IP Specification.** We evaluate whether or not rule creation specifies an individual IP as the destination.
- **Device Specification.** As IPv6 devices are often assigned multiple addresses (in some cases, one per application), creating a rule may be complicated by device/address identification. We evaluate whether rules can be created by specifying a device (e.g., by MAC address or another identifier) rather than a specific IP address.
- **IPv6 UPnP Support.** Finally, we evaluate the router's capability to offer *automatic* rule generation. Devices on the local network can use UPnP to create firewall rules programmatically if the router offers this capability.

Since routers do not explicitly advertise their firewall policies, we conduct a series of black-box scans in order to establish the default filtering model, firewall filtering policies, and hosted router services. We designed and built a custom traffic monitor on the internal host to ensure accurate collection of packets arriving through the firewall. During a scan, this monitor would listen for and record inbound IPv6 traffic with a timestamp, arrival port, protocol and scanning source IP. We reconciled the packets received with packets sent from the scanner to filter unwanted traffic and verify correct operation.

Scans were conducted using Nmap against the most common 1,000 TCP and UDP ports (as defined by the scanner). This scope was chosen due to interest in exposure of the most common ports and scan duration considerations. A complete assessment of each CE router involved nine total scans from two sources, each conducted with the firewall on and off as shown in Figure 2: First, scan (1) is conducted from the external vantage to the internal host establishing the inbound filtering strategy of the firewall. Scan (2) probes the external router interface from the external vantage to identify

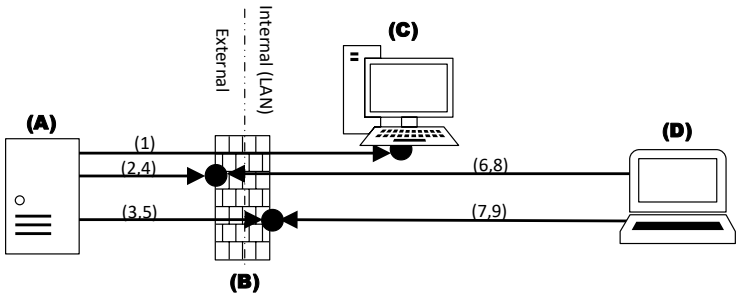

Fig. 2: **Scanning Protocol** – To fully evaluate the security policy of each router we scan from two vantage points (A) and (D) against three targets: (C) an internal host, and (B) the firewall internal and external interfaces. In total, we conducted 9 unique scans for each router.

Table 1: **Routers** – This table displays the heterogeneous nature of management options and default configurations among the devices evaluated. Bolded device names indicate that the router implements a default-permit firewall policy and IPv6 is enabled by default. Configuration options for unsupported features are marked with dashes. No device used IPv6 NAT.

Device	Brand	Firmware Version	Default IPv6	Firewall Present	Firewall Enabled	One-Click Open	Security Warning	Rule Generation	IP Specification	Device Specification	IPv6 UPnP Support
Amazon Eero	Amazon	Eero OS 3.15.2-1	○	●	●	○	○	●	○	●	○
AmpliFi Gamer's Edition	Ubiquiti	v3.3.0	○	●	●	●	●	○	–	–	●
Cisco DPC3941T XB3	Cisco	2.3.10.13_5.5.0.5	●	●	●	●	○	○	–	–	○
Google Nest (2nd Gen)	Google	12371.71.11	○	●	●	○	○	●	○	●	○
Linksys EA3500	Linksys	1.1.40.162464	●	●	●	●	○	●	●	○	○
Linksys EA6350 AC1200	Linksys	3.1.10.191322	●	●	●	●	○	●	●	○	○
Motorola MR2600	Motorola	1.0.10	●	●	○	○	○	●	●	○	○
Nighthawk X4 R7000	Linksys	1.0.0.124	○	●	●	●	○	○	–	–	○
Surfboard SBG10 DOCSIS 3.0	Arris	9.1.103AA72	●	●	●	●	○	●	●	○	○
TP-Link AC1750 v2	TP-Link	180114	●	○	–	–	○	○	–	–	○

open ports and exposed services; (3) repeats this scan on the internal interface to determine if this traditionally concealed interface is exposed under IPv6. For each interface, we conduct a banner scan against exposed ports (4 and 5). This process is repeated from the internal vantage first targeting the exposed services on each router interface (6 and 7) before conducting the same banner grab on exposed services (8 and 9). The combination of sources and targets allowed complete measurement of IPv6 filtering policies, exposure, and default operational model of the CE router. These results were then compared with our evaluation of basic router characteristics to complete a holistic router assessment, presented in Section 4: Results.

4 Results

In this section, we present the results of our experiments for each of the CE routers. In general, we find CE routers with IPv6 capability have little commonality of security implementation across manufacturers.

4.1 Operational Defaults

Table 1 presents an overview of our findings showing a wide variance in default operation, security, and user control. Eight of the ten routers assessed have an enabled default firewall policy (i.e., default-deny) for IPv6 while the remaining two devices (`TP-Link AC1750` and `Motorola MR2600`[1]) do not have a default firewall (i.e., default-permit). Neither of these two devices communicates this design decision to the consumer. At the time of writing, the `TP-Link AC1750` is Amazon US's top-selling router [1] and TP-link is the top global provider, accounting for 15.9% of all deployed devices [10], suggesting that the default permit model may be commonly deployed.

Five of these eight default deny devices further provide a "One-Click Open" option for opening the network to inbound connections. This option immediately transitions the network to a default permit model allowing all ingress traffic through to the internal hosts. The effect that this has on ingress filtering can be seen in Figure 3 in the Appendix. Only one of the ten devices evaluated provides an explicit warning to the user before allowing the firewall to be disabled using this feature. Users with minimal technical knowledge who are accustomed to a default closed model from IPv4 NAT may be unaware of the additional exposure this option creates.

Two routers, the `Motorola MR2600` and `TP-Link AC1750`, enable IPv6 routing by default with a default permit firewall. This combination of configuration settings exposes all IPv6-capable devices to the wider Internet by default. While the `Motorola MR2600` allows consumers to *optionally* enable the firewall, the user must be aware of the current state and possess the technical capability to do so. Worse, the `TP-Link` router only provides the ability to disable IPv6 and has no capability to enable any filtering.

4.2 Firewall Policies and Pinholing

We find a spectrum of firewall management options offered to the consumers ranging from subscription model services for packet inspection and filtering, to singular on/off toggles, to complete lack of firewall configuration for IPv6. Depending on the router, modifying the configuration can be accomplished through a smartphone application or a locally hosted web portal, with a few devices supporting both.

For routers that provide an interface to create exceptions to the default firewall filtering policy (pinholes), we found that two out of six connect those rules to the

[1] *Responsible Disclosure* Given the severity of enabling IPv6 support by default and a default-permit posture, we disclosed our findings to both Motorola and TP-Link in August 2020. In November 2020, Motorola issued a public patch to correct the issue. TP-Link did not respond to our disclosure.

device MAC address. We verified that in these cases, traffic destined for *any* associated address for the device is forwarded. The other four out of six routers allow users to provide a single, static address that the rule applies to; the rules are not updated if the device migrates or is assigned additional IPv6 addresses over time.

Of the routers that do not support IPv6 pinholing, only the `TP-Link AC1750` provides no ability to configure the firewall aside from disabling IPv6 (because it does not have such a firewall). For the remaining three routers, `Cisco DPC3941T XB3` also provides several options of choosing what kind of traffic is blocked besides the "One-Click Open" option, while for `Ubiquiti AmpliFi` and `Netgear Nighthawk`, *One-Click Open is the only method available for users to control the firewall.* As an example, the `Ubiquiti AmpliFi` provides users with minimal control over IPv4 policies through port-forwarding controls, but the management interface lacks an equivalent ability to create pinholes in IPv6. Ubiquiti notes this on their official FAQ: "AmpliFi does not support editing firewall configurations, and cannot be disabled unless you place the router in bridge mode" [15]. Contrary to this statement, they do allow automated modification of firewall rules through the embedded UPnP `WANIPv6FirewallControl:1` device template. For manual control, the web interface instead offers an "Allow all incoming IPv6 connections" as the only actionable solution for non-technical users.

4.3 Router Scanning

We find that when CE routers are globally accessible a majority of them expose open services to the Internet as shown by Table 2. Whether the firewalls are disabled manually or by default, six routers do not employ rules to restrict access to local network services from the global Internet. We found that services (e.g., SMTP, HTTP, and SMB) available on internal router interfaces were also offered on the external interfaces as well as the link local address on these devices. Interestingly, this indicates that the manufacturers are configuring their internal services to listen on all interfaces; when the firewall is off, these services are no longer protected. It is unclear if this is an oversight or expected operation.

We discovered two exceptional implementations: First, the `Motorola MR2600` maintains a small subset of exposed open ports on its external interface even with the firewall enabled. Second, the `TP-Link AC1750` maintains an outdated version of Dropbear SSH despite the public availability of a CVE describing a remote code execution vulnerability [13]. It is notable that, of the routers that expose ports in any firewall configuration, there appear to be a common set of ports that are open, but provide no banner. We hypothesize that these ports are associated with common services that each router provides but does not enable by default, though the ports remain open. For example, multiple routers advertise the ability to set up local storage sharing, likely using SMB on port 445. Though we did not exercise this functionality, the exposure of these ports suggests that if a client were to enable these features they would also be accessible to the wider Internet over IPv6. The default states and mix of services available provide enough unique scan data to individually identify the device manufacturer; six of the ten routers we obtain have uniquely identifying features. As a result, we believe it may be possible to fingerprint routers through probing open IPv6 ports and services, though we leave this to future work.

Table 2: **Externally Exposed Services** – This table lists the IPv6 services and open TCP ports that are exposed by each device with the firewall either enabled or disabled for the routers that support such an option. Ports in bold indicate that a service responded with a banner. We document the services associated with the address from the router's external interface. Most routers have a separate address assigned to their internal interface from their allocated subnet, though we find that the exposed services are typically the same between the two.

Device	Default FW	FW Enabled	FW Disabled
Amazon Eero	●	–	No Disable Option
AmpliFi Gamer's Edition	●	–	–
Cisco DPC3941T XB3	●	–	–
Google Nest (2nd Gen)	●	–	No Disable Option
Linksys EA3500	●	–	25, 53, **80**, 135, 139, 443, 445, **2601**, 1080, **10000**
Linksys EA6350 AC1200	●	–	25, 53, **80**, 135, 139, **443**, 445, **2601**, 1080, **10000**
Motorola MR2600	○	25, 135, 139, 445, 1080	25, 135, 139, 445, 1080
Nighthawk X4 R7000	●	–	25, 43, 80, 135, 139, 443, 445, 548, 1080, **2601**
Surfboard SBG10 DOCSIS 3.0	●	–	25, 80, 135, 139, 443, 445, 1080
TP-Link AC1750 v2	○	No Enable Option	**22**, 25, 135, 139, 445,1080

To summarize, our work shows that there is little standardization among the routers evaluated in this work around the security or operational functionality provided for IPv6 CE networks. This is in direct contrast to IPv4 where devices and services are not exposed. While NAT was not designed as a security framework, the deny-all, permit by exception ingress policy serves as an invariant for consumer routing devices and is noted as such within RFCs when debating the default recommendations of CE routers [20,3,16]. We see this argument manifest in the inconsistency between device implementations; the default policies maintained by devices put real users and systems at risk.

5 Discussion

The CE environment provides a unique challenge in balancing device capability against user ability and need. This work demonstrates that the shift to IPv6 removes the consistency of one of its most crucial layers of defense: homogeneity in router operation. Without a safe default policy, consumers must rely on the security of each of their endpoint devices, which can be difficult to ensure, especially in CE environments where device maintenance is not guaranteed. We recognize that many of these problems are not caused by or unique to IPv6 consumer networks, but we note that unclear IPv6 implementation strategies exacerbate these issues by offloading responsibility for securing and configuring the network to consumers.

We see in our assessment a struggle to shape and define what exactly is the right amount of control without under-offering or overwhelming targeted consumer demographics. This has left router manufacturers to determine what are the correct abstractions and implementations, and how to communicate these clearly to a wide demographic of users. Accordingly, we believe that addressing the general inconsistency is the most direct path to securing CE networks in IPv6.

5.1 Recommendations

There are multiple parties involved in CE environments each of which have different motivations and risk factors, but it is important that the design of CE networks prioritizes the wholesale security of consumer data and devices. We structure our recommendations around the following principles:

- The default operation mode should be secure, and the bulk of network configuration should be moved from consumers to developers.
- Configuration options should be consistent and only as permissive as necessary.
- Configuration pitfalls should have confirmation warnings that ensure users understand the risks associated with the changes they are making (*e.g.* making devices globally accessible).
- Documentation should share abstractions and language across manufacturers and be as minimally complex as feasible.

It is important to present a clear, consistent threat model to consumers whose ability and understanding often lags that of developers, to avoid oversight on responsibility for securing devices connected to home networks. This is the responsibility of both standardization bodies and the CE router industry as a whole. We strongly recommend the following defaults:

Standardization We recommend that CE routers universally standardize around a default ingress filtering policy that denies incoming traffic. We further recommend manufacturers remove or restrict the "one-click open" option on CE routers as home users are likely to unknowingly expose their whole network, violating the security principle of least privilege. If this is a required functionality, routers should warn users (and/or suggest to use IPv6 pinholing) before allowing them to use this option.

For manual exceptions we recommend that manufacturers implement both device and IP based rules and develop a consistent vocabulary for describing them. Providing users with the resources to understand when each option is preferable will require that the language used to describe IPv6 configuration options is consistent across manufacturers.

Documentation It is irrelevant what standards require if manufacturers ignore them or if parties involved fail to understand their importance or the importance of their abstractions. Fostering consumer and developer understanding of IPv6 security can create pressure on manufacturers to adhere to standards and promote transparency ahead of purchase. Establishing consistent language and abstractions for describing the security mechanisms of IPv6 networks is the first step.

Currently manufacturers of customer edge routers highlight IPv6 as an enhanced feature in their product marketing, though we found no instance of educating users about IPv6 or describing its security implications. Instead, phrases such as "provides infinite addresses for more devices", "best possible experience", and "simplifies the router's tasks" are offered as slogans to encourage user commitment [12,11]. These approaches are problematic. This hides a transparent shift in the security model of home networks that consumers cannot be expected to inherently understand on their own.

Morgner *et al.* present one possible solution of offering device label standards similar to nutrition labels on food [14]. Here, the authors focused on manufacturer guarantees for duration of product support and timeliness of updates in a standardized label. We argue to take this concept further with a holistic approach to additional aspects of security such as default configuration, control mechanisms, and 3rd party certifications. Requirements for labelling standards incentivize manufacturers to provide and document security features necessary for consumers to have a functional understanding of their network posture at purchase.

5.2 Future Work

While this work discusses at length the "One-Click Open" option, we have not conducted a formal user experience study to confirm that users will rely on this option to achieve simple routing changes in their IPv6 networks as a first choice. A proper study of the UX/UI design involved in home network security would be informative and could provide developers with a better understanding of consumer needs and approaches to IPv6 security.

While we use this work to gauge the scope of current security policies of IPv6 CE routers, a large scale examination of router IPv6 firewall behavior is required to better understand the breadth of the impact that the transition from IPv4 to IPv6 has on CE routing. Specifically, a tool assisting clients to better understand the defaults that their network implements could prove a strong contribution towards this result. Similar large scale studies of IoT and smart devices operating in IPv6 environments are reserved for future efforts as well.

6 Conclusion

In IPv4 networks, the use of NAT afforded a ubiquitous, de facto default-deny security posture. The growing deployment of IPv6, which eliminates address scarcity, no longer requires NAT. In the absence of strong guidance for how router manufacturers should implement filtering, we examined a diverse set of routers to measure real-world implementations. We find that the access control models and controls implemented to manage these networks are coarse and contain unsafe defaults that likely expose devices on the network – often without warning to the consumer. The result is a systemic, demonstrable failure among all parties to agree upon, implement and communicate consistent security policies. While IPv6 brings important advances to the Internet, significant effort by academia and industry is needed to help address and solve access control issues in the home, including adequately communicating information about these postures to consumers.

References

1. Amazon.com. Amazon Sales Popularity - Computer Routers (2020). https://web.archive.org/web/20201023233343/https://www.amazon.com/gp/bestsellers/pc/300189/ref=zg_b_bs_300189_1. Last accessed 23 Oct 2020.
2. Manos Antonakakis et al. Understanding the Mirai Botnet. In *USENIX - 26th Security Symposium*, pages 1093–1110, 2017.
3. T. Chown, J. Ed., Arkko, A. Brandt, O. Troan, and J. Weil. IPv6 Home Networking Architecture Principles. RFC 7368, Internet Engineering Task Force, October 2014.
4. Frontier Communications. Frontier Home Internet Setup Guide (2020). https://frontier.com/~/media/HelpCenter/Documents/internet/installation-setup/hsi-self-install-guide.ashx?la=en. Last accessed 18 Oct 2020.
5. Jakub J. Czyz, Matthew Luckie, Mark Allman, and Michael Bailey. Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy. In *Proceedings of the 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, San Diego, California, USA, February 2016.
6. N. De Leon. Many Wireless Routers Lack Basic Security Protections, Consumer Reports' Testing Finds. https://www.consumerreports.org/wireless-routers/wireless-routers-lack-basic-security-protections/, 2019.
7. Open Connectivity Foundation. UPnP+ Specification (2020). https://openconnectivity.org/developer/specifications/upnp-resources/upnp/#upnp-plus. Last accessed 18 Oct 2020.
8. T. Hain. Architectural Implications of NAT. RFC 2993, Internet Engineering Task Force, November 2000.
9. Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. DDoS in the IoT: Mirai and Other Botnets. *IEEE Computer*, 50(7):80–84, 2017.
10. Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. All Things Considered: An Analysis of IoT Devices on Home Networks. In *USENIX - 28th Security Symposium* , pages 1169–1185, 2019.
11. Linksys. Differences between IPv4 and IPv6 (2020). https://www.linksys.com/us/support-article/?articleNum=139604. Last accessed 18 Jun 2020.
12. Microsoft. Support: IPv6 on Xbox One (2020). https://support.xbox.com/help/Hardware-Network/connect-network/ipv6-on-xbox-one. Last accessed 18 Jun 2020.
13. MITRE. CVE-2016-7406. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7406, September 2016. Last accessed 20 Oct 2020.
14. Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products. *arXiv:1906.11094*, 2019.
15. Ubiquiti Networks. FAQ: Does AmpliFi Have a Firewall? (2020). https://help.amplifi.com/hc/en-us/articles/115009611867-Does-AmpliFi-have-a-firewall-. Last accessed 18 Oct 2020.
16. H. Singh, W. Beebee, C. Donley, and B. Stark. Basic Requirements for IPv6 Customer Edge Routers. RFC 7084, Internet Engineering Task Force, November 2013.
17. Tripwire. SOHO Wireless Router (In)Security. http://www.properaccess.com/docs/Tripwire_SOHO_Router_Insecurity_white_paper.pdf, 2014.
18. G. Van de Velde, T. Hain, R. Droms, B. Carpenter, and E. Klein. Local Network Protection for IPv6. RFC 4864, Internet Engineering Task Force, May 2007.
19. Dan Wing, Stuart Cheshire, Mohamed Boucadair, Reinaldo Penno, and Paul Selkirk. Port Control Protocol (PCP). RFC 6887, Internet Engineering Task Force, April 2013.

20. Ed. Woodyatt, J. Recommended Simple Security
Capabilities in Customer Premises Equipment (CPE) for Providing Residential
IPv6 Internet Service. RFC 6092, Internet Engineering Task Force, January 2011.
21. Lixia Zhang. A
Retrospective View of Network Address Translation. *IEEE Network*, 22(5):8–12, 2008.

7 Appendix

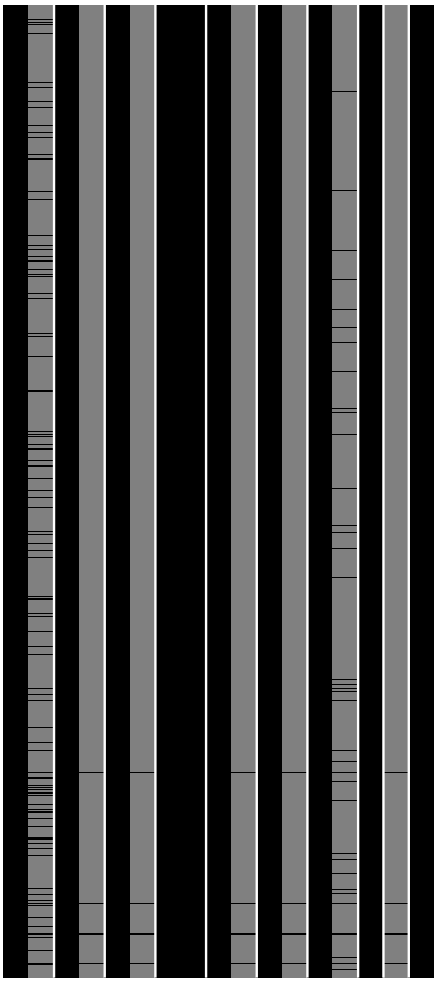

Fig. 3: **Firewall Ingress Policies (TCP)** – We use Nmap to scan the most common 1000 TCP ports on an internal host from an external vantage point. For each packet the host receives we mark the associated port GREY. Conversely, if the firewall drops the packet or the packet fails to reach the host due to network failure the associated port is marked BLACK. For routers that have an optional firewall we include a scan in both states indicated by FW or NoFW.