Egress filtering

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Egress_filtering#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Egress_filtering#searchInput)

In [computer networking](https://en.wikipedia.org/wiki/Computer_networking), **egress filtering** is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private [TCP/IP](https://en.wikipedia.org/wiki/TCP/IP) computer network to the [Internet](https://en.wikipedia.org/wiki/Internet) that is controlled.

TCP/IP packets that are being sent out of the internal network are examined via a [router](https://en.wikipedia.org/wiki/Router_(computing)), [firewall](https://en.wikipedia.org/wiki/Firewall_(computing)), or similar [edge device](https://en.wikipedia.org/wiki/Edge_device). Packets that do not meet security policies are not allowed to leave – they are denied "egress".[[1]](https://en.wikipedia.org/wiki/Egress_filtering#cite_note-1)

Egress filtering helps ensure that unauthorized or malicious traffic never leaves the internal network.

In a corporate network, typical recommendations are that all traffic except that emerging from a select set of [servers](https://en.wikipedia.org/wiki/Server_(computing)) would be denied egress.[[2]](https://en.wikipedia.org/wiki/Egress_filtering#cite_note-2)[[3]](https://en.wikipedia.org/wiki/Egress_filtering#cite_note-3)[[4]](https://en.wikipedia.org/wiki/Egress_filtering#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Egress_filtering#cite_note-5) Restrictions can further be made such that only select protocols such as [HTTP](https://en.wikipedia.org/wiki/HTTP), [email](https://en.wikipedia.org/wiki/Email), and [DNS](https://en.wikipedia.org/wiki/Domain_Name_System) are allowed. User [workstations](https://en.wikipedia.org/wiki/Workstations) would then need to be configured either manually or via [proxy auto-config](https://en.wikipedia.org/wiki/Proxy_auto-config) to use one of the allowed servers as a [proxy](https://en.wikipedia.org/wiki/Proxy_server).

Corporate networks also typically have a limited number of internal [address blocks](https://en.wikipedia.org/wiki/Subnetwork) in use. An [edge device](https://en.wikipedia.org/wiki/Edge_device) at the boundary between the internal corporate network and external networks (such as the Internet) is used to perform egress checks against packets leaving the internal network, verifying that the source [IP address](https://en.wikipedia.org/wiki/IP_address) in all outbound packets is within the range of allocated internal address blocks.

Egress filtering may require policy changes and administrative work whenever a new application requires external network access. For this reason, egress filtering is an uncommon feature on consumer and very small business networks.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Egress_filtering&action=edit&section=1)]

* [Content-control software](https://en.wikipedia.org/wiki/Content-control_software)
* [Ingress filtering](https://en.wikipedia.org/wiki/Ingress_filtering)
* [Web Proxy Autodiscovery Protocol](https://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol)

References[[edit](https://en.wikipedia.org/w/index.php?title=Egress_filtering&action=edit&section=2)]

* 1. [**^**](https://en.wikipedia.org/wiki/Egress_filtering#cite_ref-1) Robert Gezelter (1995) *Security on the Internet* Chapter 23 in Hutt, Bosworth, and Hoytt (1995) "Computer Security Handbook, Third Edition", Wiley, section 23.6(b), pp 23-12, et seq.
  2. [**^**](https://en.wikipedia.org/wiki/Egress_filtering#cite_ref-2) [*"Malware Threats and Mitigation Strategies"*](https://www.us-cert.gov/sites/default/files/publications/malware-threats-mitigation.pdf)*(PDF). Us-cert.gov. Retrieved 2015-06-20.*
  3. [**^**](https://en.wikipedia.org/wiki/Egress_filtering#cite_ref-3) [*"Holistic View of Securing IP-based Industrial Control System Networks"*](https://web.archive.org/web/20140123103348/http:/ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/S2013/Jacobs_Holistic_View_Securing_IP-based_ICS_s5.pdf)*(PDF). Ics-cert.us-cert.gov. Archived from*[*the original*](https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/S2013/Jacobs_Holistic_View_Securing_IP-based_ICS_s5.pdf)*(PDF) on 2014-01-23. Retrieved 2015-06-20.*
  4. [**^**](https://en.wikipedia.org/wiki/Egress_filtering#cite_ref-4) [*"Mitigation Monday # 2"*](https://web.archive.org/web/20150619043950/https:/www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf)*(PDF). Nsa.gov. Archived from*[*the original*](http://www.nsa.gov/ia/_files/factsheets/I733-011R-2009.pdf)*(PDF) on 2015-06-19. Retrieved 2015-06-20.*
  5. [**^**](https://en.wikipedia.org/wiki/Egress_filtering#cite_ref-5) [*"Controlling Outbound DNS Access"*](https://www.us-cert.gov/ncas/alerts/TA15-240A)*. United States Computer Emergency Readiness Team. U.S. CERT.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Egress_filtering&action=edit&section=3)]

* [RFC 3013](https://tools.ietf.org/html/rfc3013)
* [Pcisecuritystandards.org](https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf)
* [Pcisecuritystandards.org](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf)
* [Sans.org](http://www.sans.org/reading-room/whitepapers/firewalls/performing-egress-filtering-32878)

When considering best practices in [egress filtering](https://en.wikipedia.org/wiki/Egress_filtering), it is important to remember that egress filtering is not focused on protecting your network, but rather on protecting other organizations' networks. For example, the May 2017 [Wannacry Ransomware](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) attack is believed to have exploited an exposed vulnerability in the [server message block (SMB)](https://en.wikipedia.org/wiki/Server_Message_Block) protocol and was rapidly spread via communications over port 445. Egress and ingress filtering of port 445 would have helped limit the spread of Wannacry. In this post--a companion piece to [*Best Practices for Network Border Protection*](https://insights.sei.cmu.edu/sei_blog/2017/05/best-practices-for-network-border-protection.html)*,* which highlighted best practices for filtering inbound traffic*--*I explore best practices and considerations for egress filtering.

Egress filtering can be a time-consuming practice with few immediate incentives; however, when executed, this practice might have mitigated damage in a number of malicious incidents. The [2016 Dyn attack](https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/) involved infected devices sending large amounts of traffic over port 53 (DNS) to target Dyn's infrastructure. If your organization has its own DNS servers for use by internal clients, there should be no reason to allow all internal devices to send outbound traffic over port 53. This simple practice might limit the impact of similar attacks.

It is important to understand the egress filtering information flow. At a very high level, outbound traffic on a system can be considered at two levels:

* **Application Layer**. Filtering here targets communication to specific websites, including various social media applications (i.e., Facebook and Twitter).
* **Transport Layer**. Egress filtering, as discussed in this blog post, focuses on the types of protocols that you will allow outbound from your network at the network and transport layers of the [OSI model](https://en.wikipedia.org/wiki/OSI_model).

Note that, similar to our best practices in network border security, these recommendations are geared toward large organizations and government agencies and would not likely be appropriate for a home network.

Here are some things to think about as you consider implementing egress filtering:

* **Usability vs. security**. When trying to decide what to filter, it is important to understand that you will always be making a tradeoff between security and functionality and convenience for your users. Locking down your system more tightly may improve security, but you may be filtering services that users want--not just must-have services that their jobs depend on, but also conveniences that may fall into a gray area.  
    
  On the other hand, allowing users access to certain services may create risks. For example, allowing users to access public DNS resolvers, like those run by Google, could allow an external party to track your users' DNS queries. Allowing your users the ability to run certain network diagnostics to the Internet from their desktops, like ping or traceroute, could expose an organization to risks as well; the inbound ICMP reply and time-exceeded packets can be used for network mapping and for DDoS, among other things. ICMP can also be used to exfiltrate data from your network, disguising sensitive information as uninteresting control traffic.
* **Default permit or default deny?** When configuring egress filtering, your [security stance](https://en.wikipedia.org/wiki/Security_engineering#Security_stance) can either permit everything outbound by default and choose to deny specific outbound traffic, or it can deny everything by default and choose specific inbound traffic to permit.  
    
  Default deny is the more secure posture, but requires you to know about all the flow of information that needs to leave your network so you can choose what traffic to permit.  
    
  Default permit is the easier option to implement, but it can allow all sorts of unknown traffic to leave your network, which could lead to problems. When setting up a brand new network, it is more feasible to start with a default deny policy because it allows you to permit new outbound applications as needed. If you're imposing default deny egress filtering to an existing network, you run the risk of breaking needed applications you didn't know about.

**Best Practices for Egress Filtering**The following best practices for egress filtering are based on our experience helping enterprise organizations, both in the government and industrial sector, as well as on our understanding of network design, Internet operations, and the threat landscape.

* **Deploy anti-spoofing filters**. [Distributed denial of service (DDoS)](https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html) attacks often rely on sending packets with IP addresses that appear to originate from fraudulent sources, [a practice known as spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing).  
    
  Anti-spoofing filters, which prevent the outbound flow of traffic with forged source addresses from a network, help prevent the spread of deliberate malicious activity by users or malicious activity caused by infections, botnets, and other malware.  
    
  When applying filters, it is important to only allow outbound packets sourced from a block of IP addresses that belong to your network. It is also important to ensure that you are only permitting traffic sourced from your registered (Internet-routable) IP addresses.  
    
  Don't accidentally leak traffic to the Internet that has been sourced from a [private](https://en.wikipedia.org/wiki/Private_network), [request for comments (RFC)](https://en.wikipedia.org/wiki/Request_for_Comments) [1918 IP address](https://tools.ietf.org/html/rfc1918), such as the 10.x.x.x block. Such leakage will contribute to the amount of junk traffic on the Internet, and smart network operators will block traffic from RFC 1918 addresses.
* **Filter internal-only services.**Certain services don't typically need to run across the Internet and are usually reserved for internal networks. Some of those services can be associated with vulnerabilities, malicious activity, or with the leaking of sensitive data.  
    
  The decision to block these services must be made with knowledge of your network's requirements. If you need one of these services to run outbound to an external partner or vendor (such as your [cloud service provider](https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html)), you should filter the traffic to permit the service only to that partner's IP addresses.  
    
  Examples of services that should be blocked from leaving your network include:
  + MS RPC (TCP/UDP 135)
  + NetBIOS (TCP/UDP 137-139)
  + SMB (TCP 445)
  + TFTP (UDP 69)
  + Syslog (UDP 514)
  + SNMP (UDP 161-162)
* **Filter services that are often associated with malicious activity.**Consider blocking services outbound known to be used for malicious purposes rather than for business purposes. For example, consider blocking IRC (typically [TCP 6660-6669](https://www.speedguide.net/port.php?port=6669)), which is frequently used as a channel for compromised systems to speak to a command-and-control server.
* **Filter services that should be restricted to a small number of known hosts.**While certain services are critical to an organization's operation, they only need to be run from a small number of known hosts. You can filter outbound to allow only those known hosts to communicate over certain ports. This practice can prevent data exfiltration (e.g., users transmitting sensitive data disguised as DNS traffic), or users running unauthorized servers (e.g., a user running their own mail server, bypassing the security controls and filtering executed on the organization's mail server). Additionally, if you have an outbound proxy for web traffic, you might want to filter to allow only that proxy to communicate over normal web ports. Specific services to consider limiting outbound from known source IP addresses include the following:  
    
  + DNS (TCP/UDP 53)
  + SMTP (TCP 25)
  + HTTP/S (TCP 80, 443)

**Wrapping Up and Looking Ahead**

Egress filtering continues to be a challenge for the Internet community. Few incentives exist for implementing best practices beyond the satisfaction of knowing that your organization has prevented the spread of malicious activity and acted on behalf of the greater good. However, if all organizations implemented basic egress filtering, we could limit the spread of unwanted and malicious activity on the Internet, to everyone's benefit.

This article is the latest in a series of blog posts offering best practices for network security. The series is intended to help government agencies and other enterprises address hidden sources of vulnerabilities within their networks. Read our series of posts: [***Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response***](https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html), [***Six Best Practices for Securing a Robust Domain Name System (DNS) Infrastructure***](https://insights.sei.cmu.edu/sei_blog/2017/02/six-best-practices-for-securing-a-robust-domain-name-system-dns-infrastructure.html), [***Best Practices for NTP Services***](https://insights.sei.cmu.edu/sei_blog/2017/04/best-practices-for-ntp-services.html), [**Best Practices for Network Border Protection**](https://insights.sei.cmu.edu/sei_blog/2017/05/best-practices-for-network-border-protection.html)**, and**[**Best Practices for Cloud Security**](https://insights.sei.cmu.edu/sei_blog/2018/03/best-practices-for-cloud-security.html).

We welcome your feedback and suggestions for future topics regarding best practices for network security in the comments section below.

**Additional Resources**

Read all the posts in the [Best Practices in Network Security series](https://insights.sei.cmu.edu/sei_blog/best-practices-in-network-security/).

Too many network administrators think only to protect their private network resources from external attacks when assessing security threats. Today's landscape is littered with threats that emanate from malware-infected endpoints. Attackers can use these to collect and forward sensitive information from your network or to attack or spam other networks. Companies large and small are better served when network administrators are equally concerned with threats that are associated with outbound connections.  In this column, I discuss ways organizations can improve their risk profile and be better 'netizens by implementing *egress traffic filtering*.

**Filter Egress Traffic to Protect Yourself**

If you don't restrict the services that hosts in your internal networks can access, malware will inevitably find its way onto some of your hosts and may [exfiltrate data](http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/) to a location that an attacker controls. Data exfiltration could be also unintentional, i.e., an insider might incorrectly attach sensitive information an email message to upload it to a document sharing service. Sadly, data exfiltration often results from configuration error: misconfigured NetBIOS, [DNS](https://blog.icann.org/2013/12/name-collision-mitigation/), or other service traffic can leak from your trusted networks and be captured or exploited by external parties.

Irrespective of the cause, data exfiltration is a threat you can’t mitigate without egress traffic enforcement, and one you can’t readily detect if you don't [log and monitor](https://securityskeptic.typepad.com/the-security-skeptic/2013/01/-elements-of-an-effective-logging-game-plan.html) traffic behavior associated with permitted and prohibited services.

**Filter Egress Traffic to Do No Harm to Others**

In the most lax of configurations – and sadly, in many default configurations - a firewall or router may treat and forward traffic it receives from any source address as valid. Fred Avolio calls this “[The Nefarious Any](http://www.avolio.com/columns/17-TheNefariousAny.html)”. Such configurations are green fields for attacks that make use of forged source IP addresses ([IP spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing)). Compromised or unauthorized hosts that gain access to your local networks often use IP spoofing to attack ([DDoS](https://securityskeptic.typepad.com/the-security-skeptic/the-worrisome-threat-of-dns-ddos-amplification-attacks.html)) other networks, to [store child abuse](http://www.popcenter.org/problems/child_pornography/print/) or other illegal material, or to conduct [spam or phishing](http://darkwing.uoregon.edu/~joe/zombies.pdf) campaigns. This is problem enough in NAT environments: in poorly implemented router configurations, especially where you have multiple access points to the Internet, your organization can inadvertently behave as a transit network for forged, malicious traffic emanating from other organizations.

Compromised or unauthorized systems can play roles in criminal activities without the use of spoofed addresses, too. A compromised server or user device on any of your internal networks (trusted, DMZ, guest) can be used to generate spam, host malware or phishing sites. A compromised DNS name server can [host zone data](http://www.internet2.edu/presentations/jt2011summer/20110712-piscitello-domains.pdf) for a malicious domain. Improperly configured, your DNS resolver – or possibly any UDP-based service you use ([chargen](https://www.cert.be/docs/chargensnmp-ddos-attacks-rise), [NTP](https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks)) - can support a [criminal conspiracy](https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/)!

Just as egress traffic filtering can help mitigate data exfiltration from your networked assets, so can it help you [protect the world from your network](https://securityskeptic.typepad.com/the-security-skeptic/2013/04/protecting-the-world-from-your-network.html).

**Step #1: Egress Traffic Enforcement Policy**

Motivated? Good. Begin by consulting your company's Security Policy and/or Acceptable Use Policy (AUP). If you don't have such policies, gather stakeholders and define them. Include as stakeholders individuals who are not only responsible for implementing your company's network security but also those individuals who are party to risk management and mitigation. Without clearly-defined notions of network security and a strict application and traffic policy you intend to enforce, your firewall configuration will end up being little more than an ad hoc and troublesome listing of outbound rules to meet users' perceived needs, instead of a well conceived policy designed to protect the company's resources.

Compose a list of the approved Internet-accessible services. For an organization that outsources email and DNS, this list might include DNS, POP/IMAP, SMTP, NTP, and HTTP/HTTPS. Think, too, about malicious destinations - botnet C&Cs, [hijacked address space](https://securityskeptic.typepad.com/the-security-skeptic/2011/06/internet-address-hijacking-spoofing-and-squatting-attacks.html), notorious ([bad](http://hostexploit.com/)) hosting providers - and how you might block these.

If your organization supports services like email and DNS from its own internal servers, compose a list of these services and service hosts (domain names and IP addresses). List any Internet servers these must communicate with. If, for example, you run a split-DNS then include any public servers your DNS server contacts for zone transfers, uses as resolvers, etc. If you run SMTP, include any mail servers with which you exchange mail directly (typically, your ISP's mail hosts). If you intend to implement *content exit control* at a proxy or firewall, enumerate the types of content you will permit or deny. You many also find it necessary to identify permission sets for user groups if your content exit control is not a "one glove fits all" policy.

Accept the fact that your firewall configuration will deviate from the ideal enforcement policy you develop following this exercise. Such deviations or exceptions may be necessary to accommodate senior management, business relationships, or sometimes for lack of a better or more secure path to completing a critical project. Assess the risk of each deviation, call attention to the security risks inherent in any alteration you are required to make to the firewall's egress policy, and consider how you might compensate by implementing a complementary security measure.

**Step #2: Kill the Nefarious ANY**

The best way to configure egress traffic filtering policies is to begin with a DENY ALL outbound policy, packet filter, or firewall rule. This creates a "nothing leaves my network without explicit permission" security baseline. Next, add rules to allow authorized access to the external services identified in your egress traffic enforcement policy. Add granular, restrictive rules to allow administrators access to network and security systems outside your firewall. Lastly, add rules to allow servers you operate from your trusted network to communicate with Internet-hosted servers.

Let's examine each of these general policies in some detail.

**Restrict Internet Access to Authorized Sources**

In many firewalls, the default egress traffic policy for trusted networks is to allow any source address in outbound packets: literally, if the source address is syntactically correct, your firewall will forward it. This is overly permissive for any network, large or small. Prune it. List the IP subnet numbers or individual IP addresses of hosts that are authorized (trusted) to make use of externally hosted services.

Limit the addresses allowed to send traffic to Internet destinations by configuring policies such as these:

* **Block IP spoofing**. Only allow source addresses from the IP network numbers you assign to internal networks to pass through your firewall (trusted, DMZ, guest). This includes primary and secondary network numbers, and subnets that are routed to the Internet through your firewall (including addresses reserved for VPN clients).
* **Only allow traffic from address space you actually use**. Apply appropriate subnet masks to internal networks, i.e., masks that are sufficiently long to identify only that fragment of the IP network number that you are using. For example, if you are using an [RFC 6761](https://tools.ietf.org/html/rfc6761) Private Address from 172.16.0.0 and only assigning numbers from 172.16.1.x, use 255.255.255.0 (or /24) and not 255.255.0.0 (or /16) as your subnet mask. (Same rule applies for [RFC 4913](https://tools.ietf.org/html/rfc4193) Private addresses for IPv6.
* **Block traffic from any RFC 6761 or RFC 4913 private addresses** from being forwarded over your Internet access circuit. Many ISPs block incoming traffic containing private addresses but you're forcing your ISP to process traffic you ought to block.
* **Block outbound traffic from VLAN workgroups** or entire network segments that has no business establishing client connections to Internet servers.
* **Block broadcast traffic**. Most Internet-facing firewalls operate in routed mode where broadcasts will not pass across LAN segments. Understand the [implications](http://etherealmind.com/11-things-about-using-a-transparent-or-layer-2-firewall/) (limitations?) of using transparent (layer 2) firewalls in Internet firewall deployments.
* **Block all outbound traffic from internal servers that have no business establishing client connections to destinations outside your trusted networks**. An example might be an intranet server that relies entirely on internally provided services (DNS, mail, time, etc.) and by design uses no applications that require Internet access.
* **Block outbound traffic with destinations that are listed on**[**DROP**](http://www.spamhaus.org/drop/)**(Don’t router or peer) or BGP filter lists**. Spamhaus, for example, maintains lists of networks that have been hijacked by spammers, phishers, botnet C&C’s and other malicious traffickers. Data centers, universities, and large end user networks especially benefit from this kind of filtering when their ISPs do not implement them.

**Restrict Internet-Accessible Services (Destinations)**

The Nefarious ANY appears again in the default egress traffic policy of firewalls that allow hosts on internal networks to access any service (port) on Internet hosts if forwarding to the destination is permitted.

Limit the destination ports on Internet-directed traffic in the following ways:

* **Only allow outbound connections to those services your egress traffic enforcement policy allows.**
* **Only allow client hosts to access authorized services from authorized external servers**. If your employees use your ISP for email services, for example, limit outbound SMTP and POP connections to your ISP's POP and SMTP servers.
* **Only allow client hosts to send DNS queries to resolvers you manage or**[**responsibly managed open resolvers**](https://securityskeptic.typepad.com/the-security-skeptic/2014/01/harden-you-recursive-resolvers-for-you-and-for-everyone-else.html).  Open resolvers are routinely exploited in DDoS attacks: [harden your resolvers](https://securityskeptic.typepad.com/the-security-skeptic/2014/01/harden-you-recursive-resolvers-for-you-and-for-everyone-else.html) and don't use others that operate "open" badly.
* For inter-server communications involving external servers, **only allow access to service ports your internal servers must use to operate correctly**. If you operate your own mail servers, make certain that only these servers establish outbound SMTP connections.
* If you operate an HTTP proxy, or a proxy system that performs some form of web URL or content filtering, **only allow outbound connections through your firewall from the proxy(ies)**.
* If you provide DNS internally, or use a split DNS, **use internal resolvers as forwarders for your internal networks**. If you make use of a private namespace that is not delegated from the public DNS, consider measures to prevent private name space queries from leaking into the public DNS (hard) or [use a FQDN](https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf) (fully qualified domain) for your private name space.
* **Block routing protocols at your firewall**. This is important for large enterprises with multiple firewalls and Internet access routers as well as small businesses with broadband connections that use a firewall to exchange and negotiate PPP over Ethernet (PPPoE). If your firewall is participating in external routing, make certain your advertisements correctly enumerate your IP networks.
* If you authorize services that make use of unique ports for remote desktop, subscription, licensing channels (e.g., GoToMyPC, BackWeb, Microsoft),  only allow access to these services from hosts that are authorized to use them.

**Testing and Monitoring Egress Traffic Policies**

Firewall configuration testing remains an acquired skill, effectively performed by firewall experts, auditors or security professionals with this special expertise. Because many egress traffic-handling policies will be source address dependent, you can achieve some confidence that your configuration satisfies your policies by logging intensely, running address and port scanning tools, and confirming that your allow/deny results are what you expect. Rigorous logging of denied outbound connections could help identify scofflaws that are either ignorant or defiant of your AUP, as well as provide early warning of infections. Where possible, cause potentially dangerous denied outbound packets to trigger notification for further investigation. Consider, too, tools like [ftester](http://dev.inversepath.com/trac/ftester) (now deprecated but still available), [NMAP](https://nmap.org/), [Nessus](http://www.nessus.org/), or some of the commercial software listed at [Security Wizardry](http://www.securitywizardry.com/index.php/products/Firewalls/Firewall-Rule-Editors-and-Testers.html) if you are looking for automated alternatives.

**Conclusion**

When I first wrote this article with Nathan Buff in 2003 we concluded that configuring egress traffic policies is admittedly more time consuming than not, and that your organization should rightly assess whether the time invested and the improved risk profile you achieve when you take this initiative is justified. This was perhaps too soft a sell. Events throughout the past 18 months (2013-2014) bear evidence that motives to exfiltrate data will only increase. I now believe that governments and private organizations are near the tipping point and no longer willing to passively accept the current threat condition but now actively investigating ways to mitigate harm resulting from the lax security practices of others. It may only be a small matter of time before [regulatory compliance](http://www.informationweek.com/security/attacks-and-breaches/ddos-attack!-is-regulation-the-answer/d/d-id/1114050) or fear of being held [contributory](http://resources.infosecinstitute.com/legality-ddos-criminal-deed-vs-act-civil-disobedience/) to a criminal act or liable for financial loss will drive many organizations to choose to implement stringent egress traffic policies.

Use the time wisely.

The original (2003) version of this article can be found [here](https://securityskeptic.typepad.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering-2003.html).

**Ingress & Egress Filtering Lab**

**Campus Network Design & Operations Workshop**

**Introduction**

These exercises will show important IP filtering techniques that significantly improve the security of your network, and the whole Internet, by preventing IP packets with “spoofed” source addresses from either entering or leaving your AS. For a more complete explanation of these concepts, see IETF’s [BCP 38](http://www.ietf.org/rfc/rfc2827.txt) and [BCP 84](http://www.ietf.org/rfc/rfc3704.txt) documents.

**Outbound Packet Filtering**

Traffic leaving your campus should not have source IP addresses which are not part of your campus public IP address space:

On your Border router:

ip access-list extended to-nren

remark Permit NREN point to point link subnet

permit ip 100.68.0.Y 0.0.0.3 any

remark Permit Campus X public IPv4 address block

permit ip 100.68.X.0 0.0.0.255 any

remark Deny any other sources

deny ip any any

!

interface FastEthernet0/0

ip access-group to-nren out

!

Do the same for IPv6:

ipv6 access-list to-nren-v6

remark Permit NREN point to point link subnet

permit ipv6 2001:DB8:100:X::/127 any

remark Permit Campus X public IPv6 address block

permit ipv6 2001:DB8:X::/48 any

remark Deny any other sources

deny ipv6 any any

!

interface FastEthernet0/0

ipv6 traffic-filter to-nren-v6 out

!

**Inbound Packet Filtering**

Traffic received from outside your campus should never be sourced from IP addresses that belong to your campus.

On your Border router:

ip access-list extended from-nren

deny ip 100.68.X.0 0.0.0.255 any

permit ip any any

!

interface FastEthernet0/0

ip access-group from-nren in

!

Do the same for IPv6:

ipv6 access-list from-nren-v6

deny ipv6 2001:DB8:X::/48 any

permit ipv6 any any

!

interface FastEthernet0/0

ipv6 traffic-filter from-nren-v6 in

!

**Management VLAN filtering**

In the Layer2 labs, we created a management VLAN for managing the switches (SSH, SNMP, etc. ). In order to protect that network from malicious access, you will need to implement filtering at the router level.

Here we assume that the NOC subnet is 100.68.X.128/28.

On your Core router:

ip access-list extended to-mgmt

permit ip 100.68.X.128 0.0.0.15 any

deny ip any any

!

interface Vlan 10

ip access-group to-mgmt out

!

interface Vlan 20

ip access-group to-mgmt out

!

Do the same for IPv6:

ipv6 access-list to-mgmt-v6

permit ipv6 2001:DB8:X:3::/64 any

deny ipv6 any any

!

interface Vlan 10

ipv6 traffic-filter to-mgmt-v6 out

!

interface Vlan 20

ipv6 traffic-filter to-mgmt-v6 out

!

Check connectivity to the Management subnet. Are you able to access the Management addresses for the building switches from the Border and Core routers now?

What about access from the Management subnets of the switches out to the Internet? Are you able to explain to the instructors what is happening now?

**Appendix - More Sophisticated Campus Filters**

This appendix looks at some of the possible filtering strategies for campuses looking to secure their infrastructure from some of the more common vulnerabilities targeted by worms and other malicious software on compromised systems connected to the Internet.

If you still have time in the class, try them out on your Campus Border Router by adding them on to what you already have configured.

**Filters**

The following list is a common list of filters that many operators install on their border routers, both inbound and outbound. The list can be applied to IPv4 and IPv6, and inbound as well as outbound on the external interface. Don’t forget for IPv6 to allow the Link Local address block, otherwise IPv6 will not work between your router and your NREN.

deny tcp any any eq 23 ! block telnet - insecure

deny udp any any eq 69 ! block TFTP - never seen from outside

deny udp any any range 135 139 ! netbios stuff

deny tcp any any range 135 139 ! netbios stuff

deny tcp any any eq 445 ! Blaster worm

deny udp any any eq 514 ! SYSLOG - never seen from outside

deny tcp any any eq 1025 ! Microsoft RPC exploit

deny tcp any any eq 1337 ! Redshell backdoor

deny tcp any any eq 1433 ! MS SQL worm

deny udp any any eq 1434 ! MS SQL worm

deny udp any any eq 2049 ! Sun NFS

deny tcp any any eq 2745 ! Blaster worm

deny tcp any any eq 3001 ! NessusD backdoor

deny tcp any any eq 3127 ! MyDoom! worm

deny tcp any any eq 3128 ! MyDoom! worm

deny tcp any any eq 5000 ! WindowsXP UPnP port

deny tcp any any eq 6129 ! Dameware backdoor

deny tcp any any eq 11768 ! Dipnet/Oddbob worm

deny tcp any any eq 15118 ! Dipnet/Oddbob worm

The following is extremely useful and is only applied to **inbound** filters:

permit tcp any any established ! only allow established TCP connections

This would be applied **first** in the inbound packet filter to only allow the return packets from outbound TCP sessions. It will not allow any remote site to initiate an incoming TCP connection. For that, a specific entry in the packet filter matching that TCP port will be required. It’s a very powerful and necessary filter line for a campus border router.

**Other ports to block**

You may want to consider blocking other ports too. Here are some examples:

* Do you run a web server on campus? If so, is it using https (tcp/443) with certificate generated by Letsencrypt? Or are you still using http (tcp/80)? So maybe only allow port 80/443 to known web servers, so as not to create the opportunity for vulnerabilities if any end users accidentally start up a web server on their computing device (applies to those using public IP address space).
* Only allow NTP to devices acting as NTP sources for the campus (consult the Campus Best Operations Practices presentation for more details).
* Incoming and outgoing email using SMTP (tcp/25) should only use your official SMTP servers. Blocking SMTP for the rest of the campus address space is strongly recommended. Users sending email via third party relays will be using tcp/465 or tcp/587, never tcp/25.

There are many more examples. Discuss with your colleagues in your group.

**Ports and Services never to block**

There are also ports and services never to block:

* ICMP - Internet Control Message Protocol
* SSH and VPNs - end users will want to use Secure Shell to connect to remote R&E institutions and other sites.
* All of UDP - this will break name lookups using the DNS. Even allowing DNS and blocking everything else UDP in the hope that peer-to-peer traffic will be blocked just will mean that peer-to-peer will use TCP instead (which a lot of it is doing these days anyway).