Network Infrastructure
Filtering at the border

Acknowledgement

- Original slides prepared by
  - Merike Kaeo
  - Fakrul Alam <fakrul@bdhbu.com>
  - Yoshinobu Matsuzaki <maz@iij.ad.jp>

What we have in network?

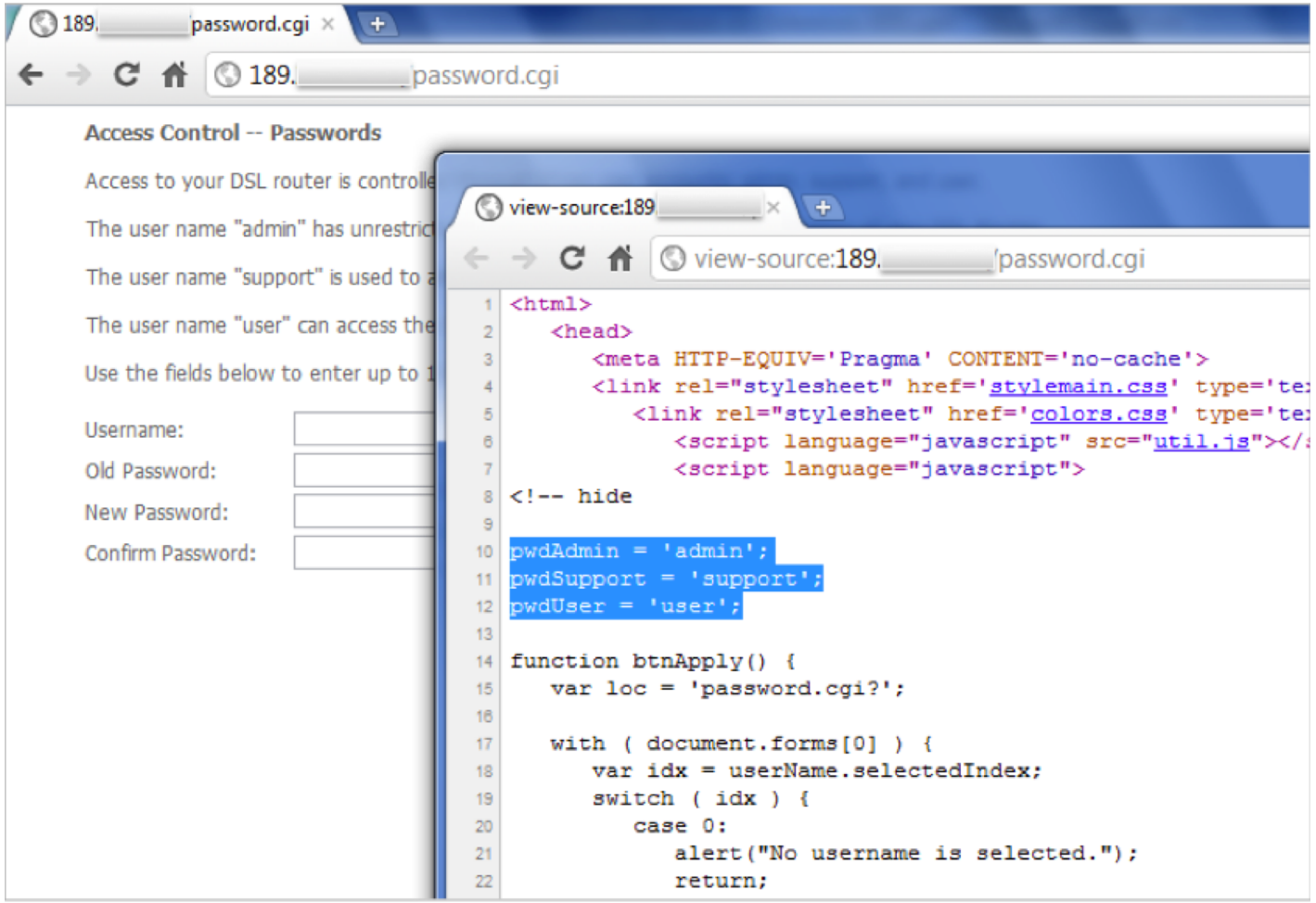
- Router
- Switch
- CPE (Home Router / WiFi Router)
- Servers
- PC/Laptop
- Smart Phone

Securing The Device

Think of ALL Devices

- The following problem was recently reported and affects low-end CPEs (ADSL connections only)
  - Admin password exposed via web interface
  - Allow WAN management (this means anyone on Internet)
  - Bug fixed and reintroduced depending on the firmware version
- The bug is quite a number of years old

Password Visible via Web Interface



MIRAI

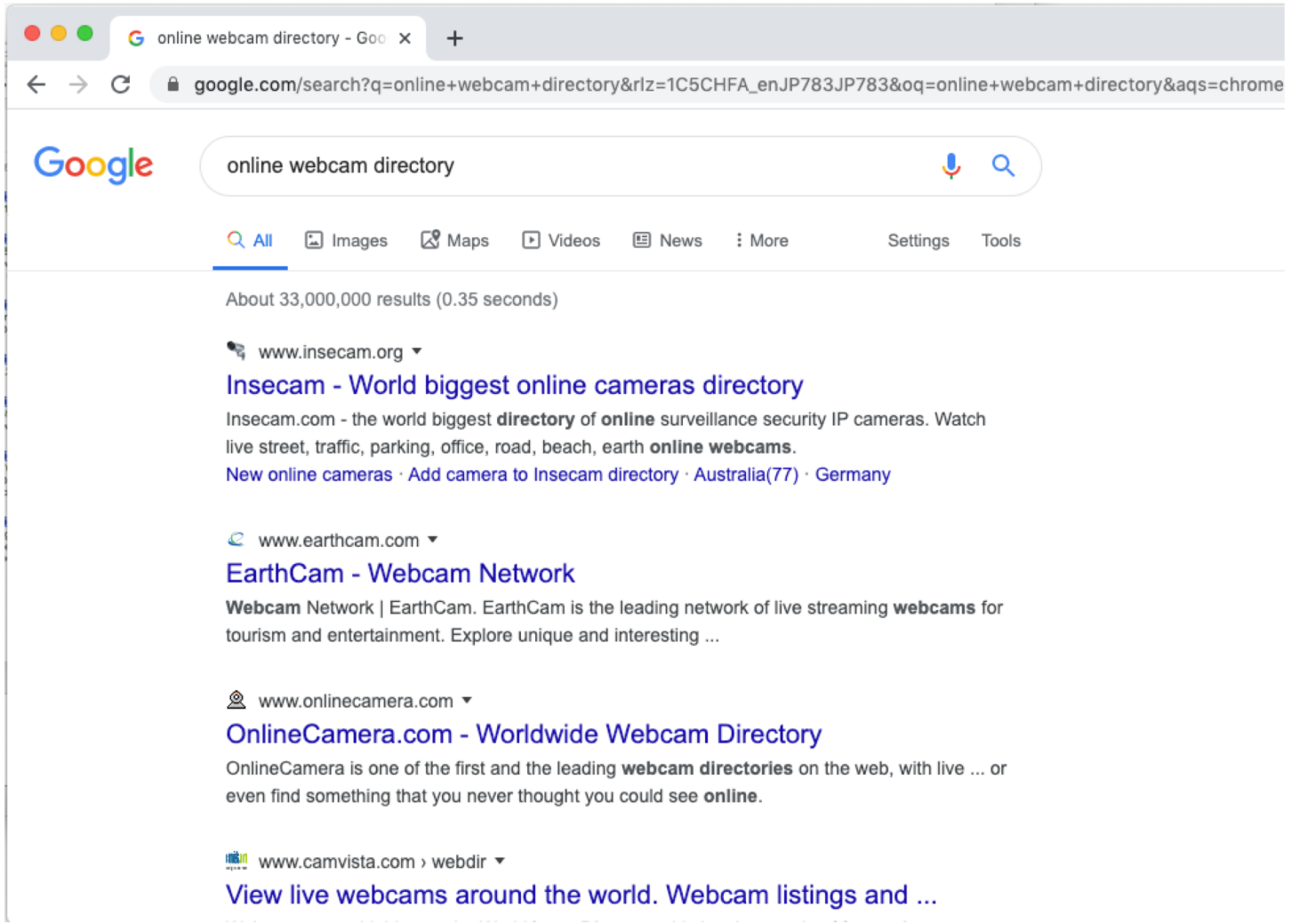
- MIRAI is one of the famous virus spread in 2016
- Random attack using “default” usernames/passwords to login
- Scan other devices once affected
- Affected devices were used for DDoS
- Source code was disclosed, and many variants appeared
- A research paper[*] estimated that 600,000 devices were infected at maximum

[*] Manos Antonakakis, et al., “Understanding the Mirai Botnet”, 26th USENIX Security Symposium, 2017.

IoT Devices may be weaker

- People are careless on managing home routers/IoT devices
- Not enough support for security fixes (especially for cheap products)
- Can run many years having potential security vulnerabilities

Finding out open IPcam!!!



Smarter devices, smarter attackers

- Smart phone attack
  - https://www.us-cert.gov/ncas/current-activity/2019/08/27/apple-releases-multiple-security-updates
- Remote Desktop
  - https://support.citrix.com/article/CTX267027
- Cable Modem attack
  - https://cablehaunt.com

Could device hardening have made a difference?

Device Access Control (Physical)

- Lock up the server room. Equipment kept in highly restrictive environments
- Set up surveillance
  - log access authorizations, set up video cameras
- Make sure the most valuable and vulnerable devices are in that locked room
- Keep intruders from opening the case
  - Easier to leave with a hard-drive than the tower
- Protect the portables
  - They are easy to steal
  - Put them in locked closet or safe when they are not with you
  - Use full disk encryption, biometric readers, and software that "phones home" if the stolen laptop connects to the Internet

Device Access Control (Physical)

- Pack up the backups
  - They should be locked in a drawer or safe, preferably off-site
- Disable the drives
  - USB ports, other external means to connect a device
- Social engineering training and awareness
- Console access
  - password protected
  - access via OOB (Out-of-band) management
  - configure timeouts

Device Access Control (Logical)

- Set passwords to something not easily guessed
- Use single-user passwords (avoid group passwords)
- Encrypt the passwords in the configuration files
- Use different passwords for different privilege levels
- Use different passwords for different modes of access
- IF AVAILABLE – use digital certificate based authentication mechanisms instead of passwords

Management Plane Filters

- Authenticate Access
- Define Explicit Access To/From Management Stations
  - SNMP
  - Syslog
  - TFTP
  - NTP
  - AAA Protocols
  - SSH, Telnet, etc.

Turn Unused Services Off

Feature	Description	Default	Recommendation	Command
TCP small servers	Standard TCP network services: echo, chargen, etc	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly	no service tcp-small-servers
UDP small servers	Standard UDP network services: echo, discard, etc	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly	no service udp-small-servers
Finger	Unix user lookup service, allows remote listing of logged in users.	Enabled	Unauthorized persons don’t need to know this, disable it.	no service finger
HTTP server	Some Cisco IOS devices offer web-based configuration	Varies by device	If not in use, explicitly disable, otherwise restrict access	no ip http server

Turn Unused Services Off

Feature	Description	Default	Recommendation	Command
Bootp server	Service to allow other routers to boot from this one	Enabled	This is rarely needed and may open a security hole, disable it	no ip bootp server
PAD Service	Router will support X.25 packet assembler service	Enabled	Disable if not explicitly needed	no service pad
Proxy ARP	Router will act as a proxy for layer 2 address resolution	Enabled	Disable this service unless the router is serving as a LAN bridge	no ip proxy-arp
IP directed broadcast	Packets can identify a target LAN for broadcasts	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it	no ip directed-broadcast

Fundamental Device Protection Summary

- Secure logical access to routers with passwords and timeouts
- Never leave passwords in clear-text
- Authenticate individual users
- Restrict logical access to specified trusted hosts
- Allow remote vty access only through ssh
- Disable device access methods that are not used
- Protect SNMP if used
- Shut down unused interfaces
- Shut down unneeded services
- Ensure accurate timestamps for all logging
- Create appropriate banners
- Test device integrity on a regular basis

Securing The Data Path

Securing The Data Path

- Filtering and rate limiting are primary mitigation techniques
- Edge filter guidelines for ingress filtering (BCP38/BCP84)
- Null-route and black-hole any detected malicious traffic
- Netflow is primary method used for tracking traffic flows
- Logging of Exceptions

Data Plane (Packet) Filters

- Most common problems
  - Poorly-constructed filters
  - Ordering matters in some devices
- Scaling and maintainability issues with filters are commonplace
- Make your filters as modular and simple as possible
- Take into consideration alternate routes
  - Backdoor paths due to network failures

Filtering Deployment Considerations

- How does the filter load into the router?
- Does it interrupt packet flow?
- How many filters can be supported in hardware?
- How many filters can be supported in software?
- How does filter depth impact performance?
- How do multiple concurrent features affect performance?
- Do I need a standalone firewall?

General Filtering Best Practices

- Explicitly deny all traffic and only allow what you need
- The default policy should be that if the firewall doesn't know what to do with the packet, deny/drop it
- Don't rely only on your firewall for all protection of your network
- Implement multiple layers of network protection
- Make sure all of the network traffic passes through the firewall
- Log all firewall exceptions (if possible)

Filtering Recommendations

- Log filter port messages properly
- Allow only internal addresses to enter the router from the internal interface
- Block packets from outside (untrusted) that are obviously fake or commonly used for attacks
- Block packets that claim to have a source address of any internal (trusted) network.

Filtering Recommendations

- Block incoming loopback packets and RFC 1918 networks
  - 127.0.0.0
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.0.0
  - 192.168.0.0 – 192.168.255.255
- Block multicast packets (if NOT using multicast)
- Block broadcast packets (careful of DHCP & BOOTP users)
- Block incoming packets that claim to have same destination and source address

special IPv4 addresses

Description	Network
default	0.0.0.0/8
loopback	127.0.0.0/8
RFC 1918	10.0.0.0/8
RFC 1918	172.16.0.0/12
RFC 1918	192.168.0.0/16
TEST-NET-1	192.0.2.0/24
TEST-NET-2	198.51.100.0/24
TEST-NET-3	203.0.113.0/24
benchmark	198.18.0.0/15
ISP shared	100.64.0.0/10
IPv4 link local	169.254.0.0/16

Example Incoming IPv4 Bogon Packet Filter

```
ip access-list extended IPv4-deny-Bogons
 deny   ip 0.0.0.0 0.255.255.255 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 deny   ip 192.0.2.0 0.0.0.255 any log
 deny   ip 198.51.100.0 0.0.0.255 any log
 deny   ip 203.0.113.0 0.0.0.255 any log
 deny   ip 198.18.0.0 0.0.1.255 any log
 deny   ip 100.64.0.0 0.63.255.255 any log
 deny   ip 169.254.0.0 0.0.255.255 any log
 deny   ip 224.0.0.0 15.255.255.255 any log
 permit ip any any
```

See http://www.team-cymru.org/bogon-reference.html for an up-to-date list

This list is dynamic. You may not want to built filters without checking the list manually first.

RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

Guideline for BCP38

- Networks connecting to the Internet
  - Must use inbound and outbound packet filters to protect network
- Configuration example
  - Outbound—only allow my network source addresses out
  - Inbound—only allow specific ports to specific destinations in

Techniques for BCP38

- Static ACLs on the edge of the network
- Unicast RPF strict mode

Example of Packet Filter

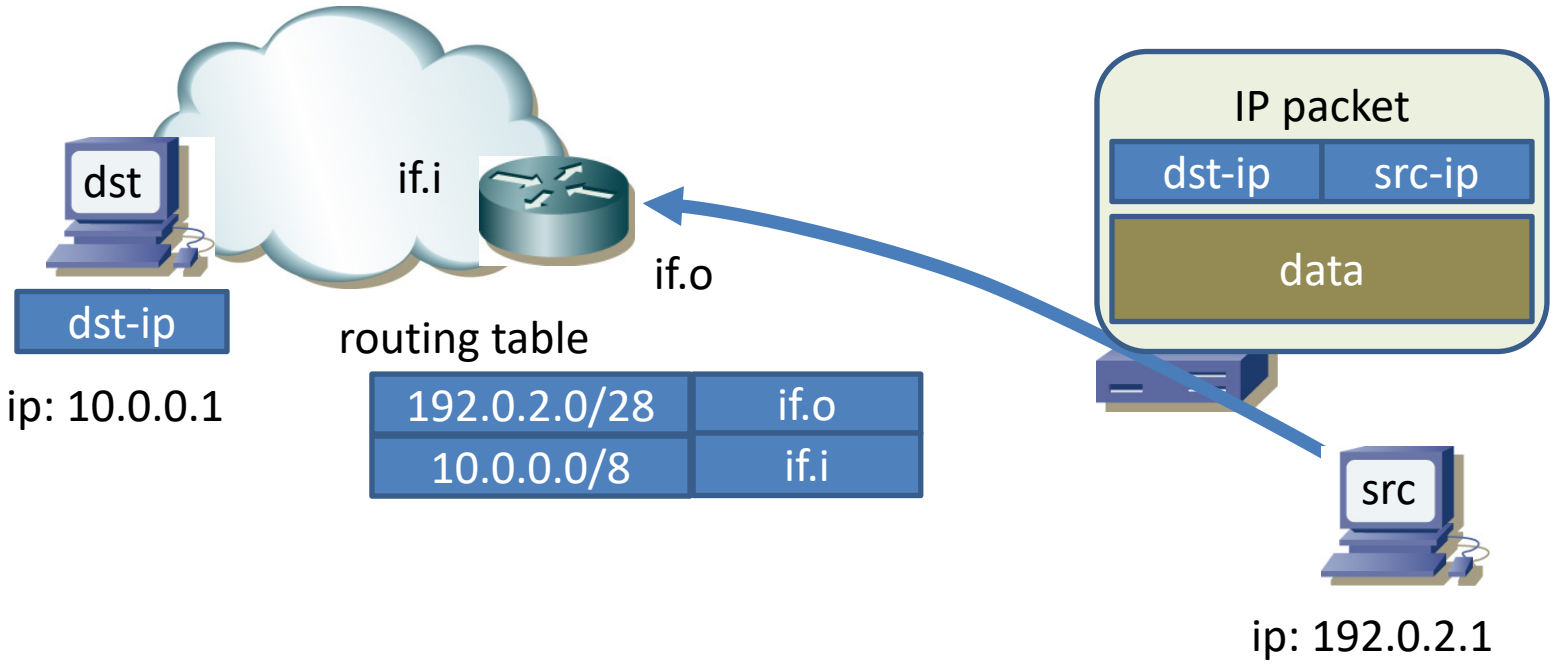
```
access-list 121 permit ip 192.168.1.250 0.0.0.255 any
access-list 121 deny ip any any log
!
interface Fastethernet0
    Description Link to our LAN
    ip access-group 121 in
```

uRPF strict mode

```
interface Fastethernet0
    Description Link to our LAN
    ip verify unicast source reachable-via rx
```

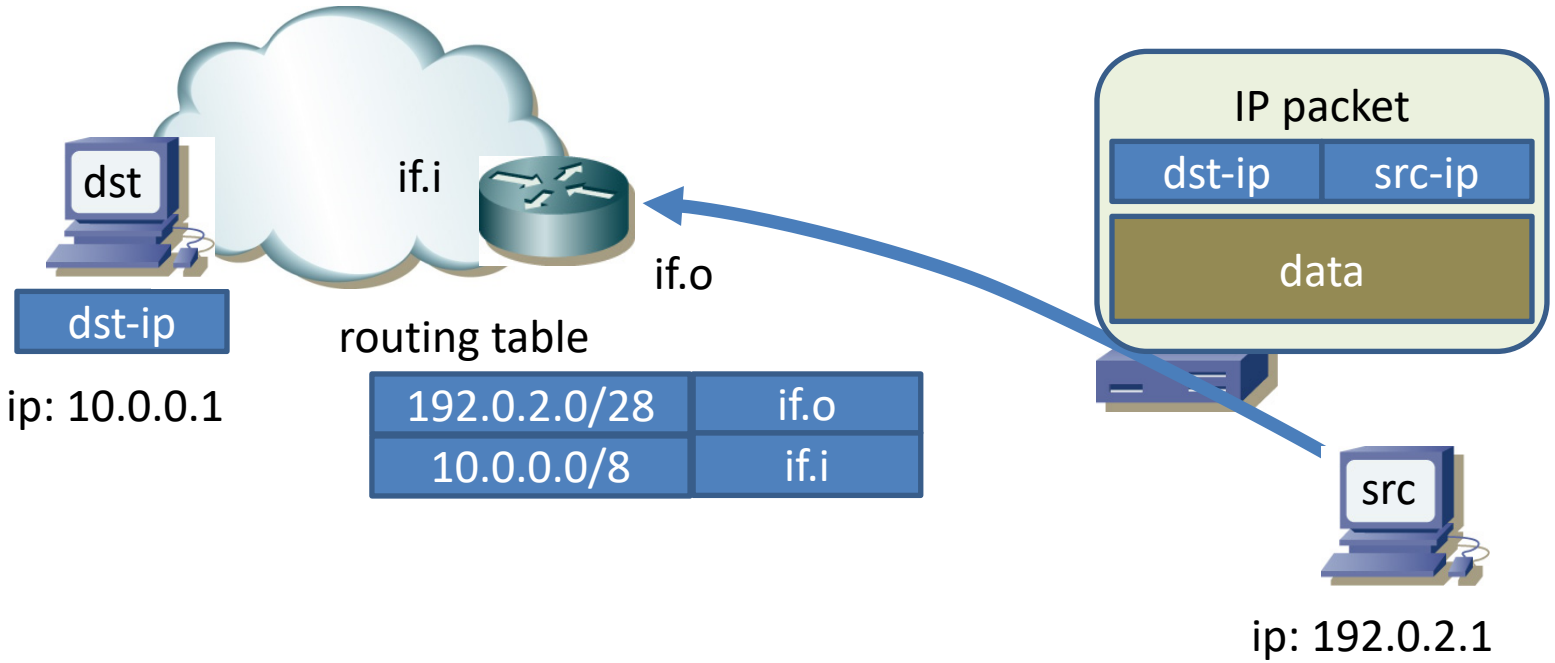
packet forwarding – dst-ip based

- routing_table(dst-ip) => outgoing interface
  - lookup by 10.0.0.1 => if.i
  - then router forwards the packet

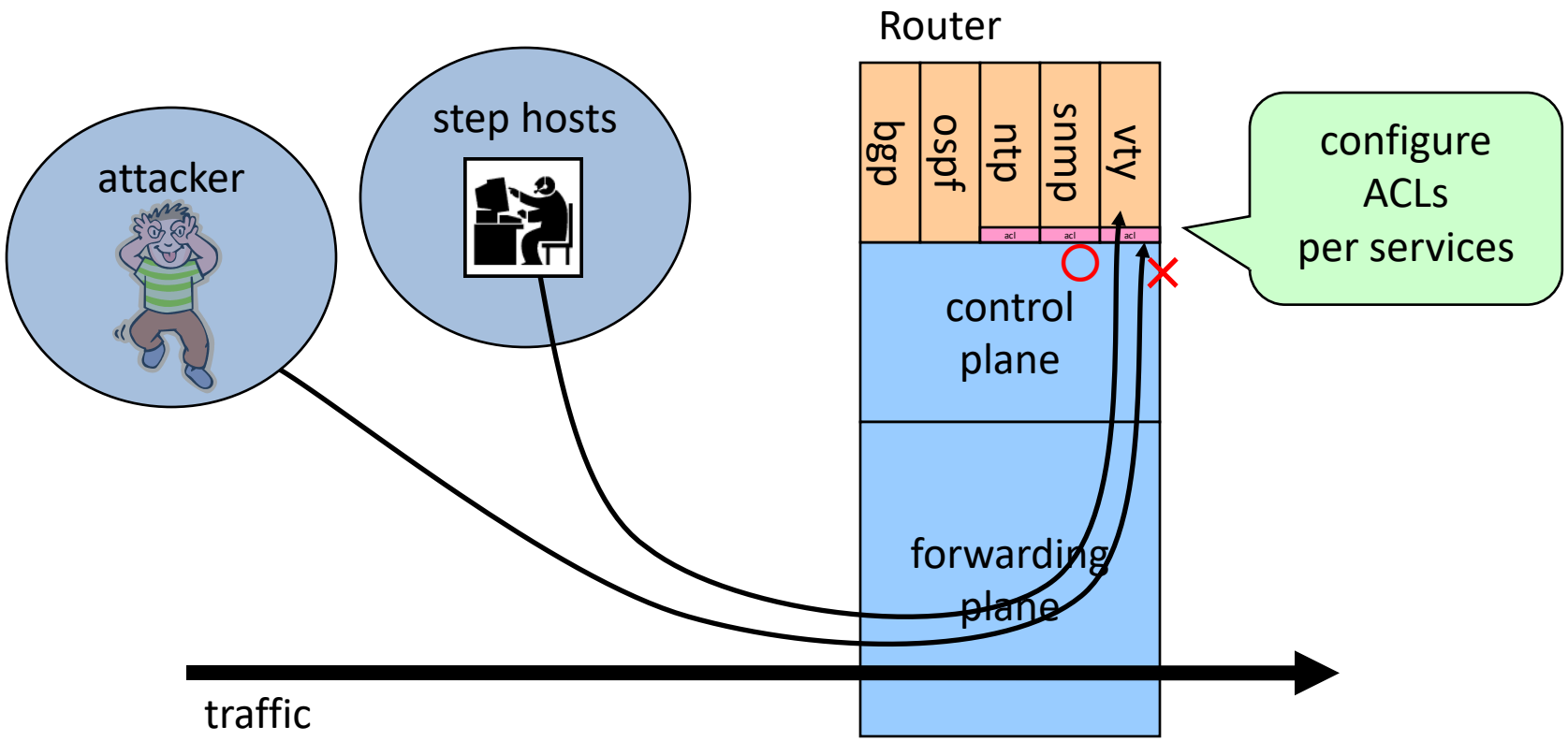


uRPF – lookup by the src-ip

- routing_table(src-ip) => interface
  - lookup by 192.0.2.1 => if.o
  - The result MUST match the incoming interface

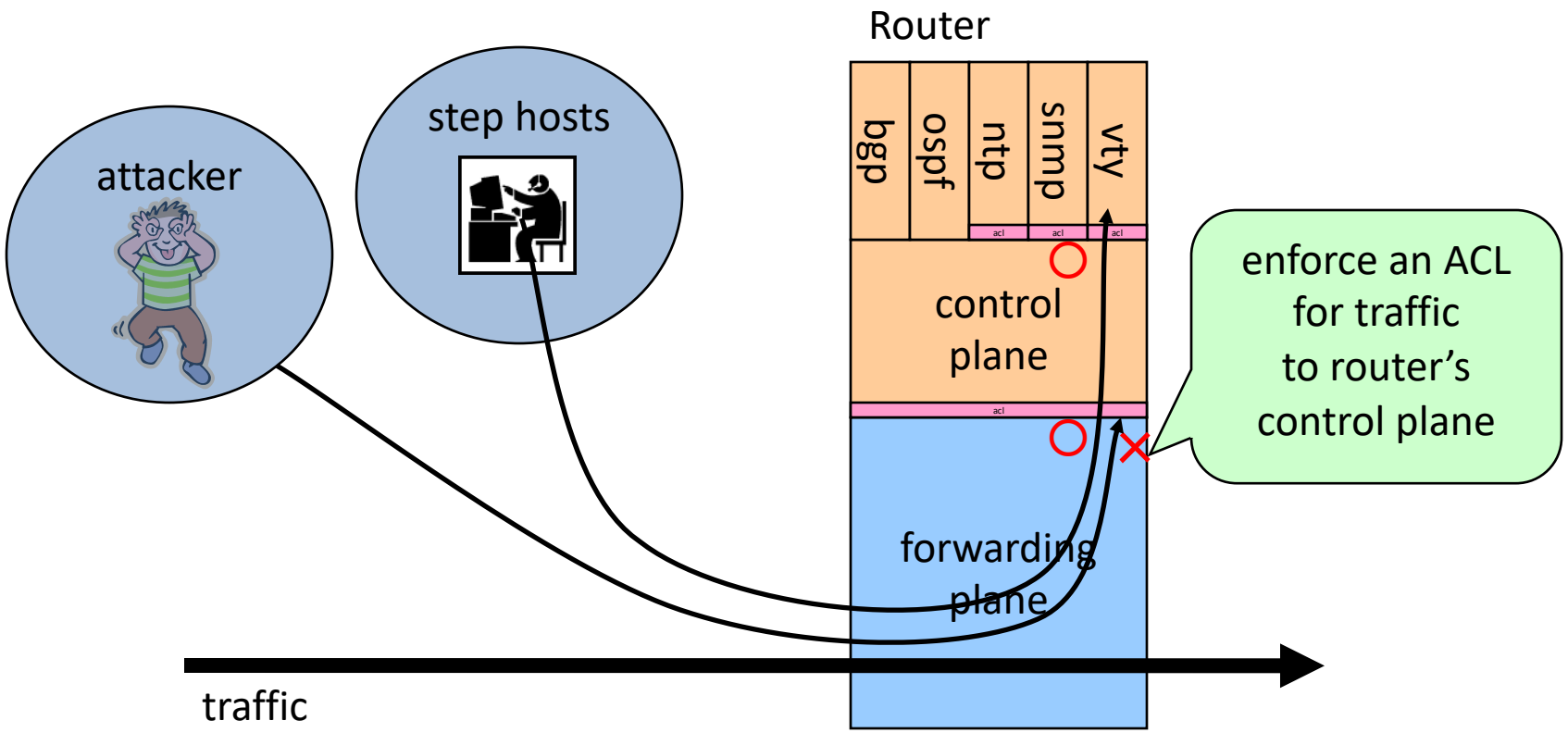


access control per services



Received/Router ACL (rACL)

access control against control plane

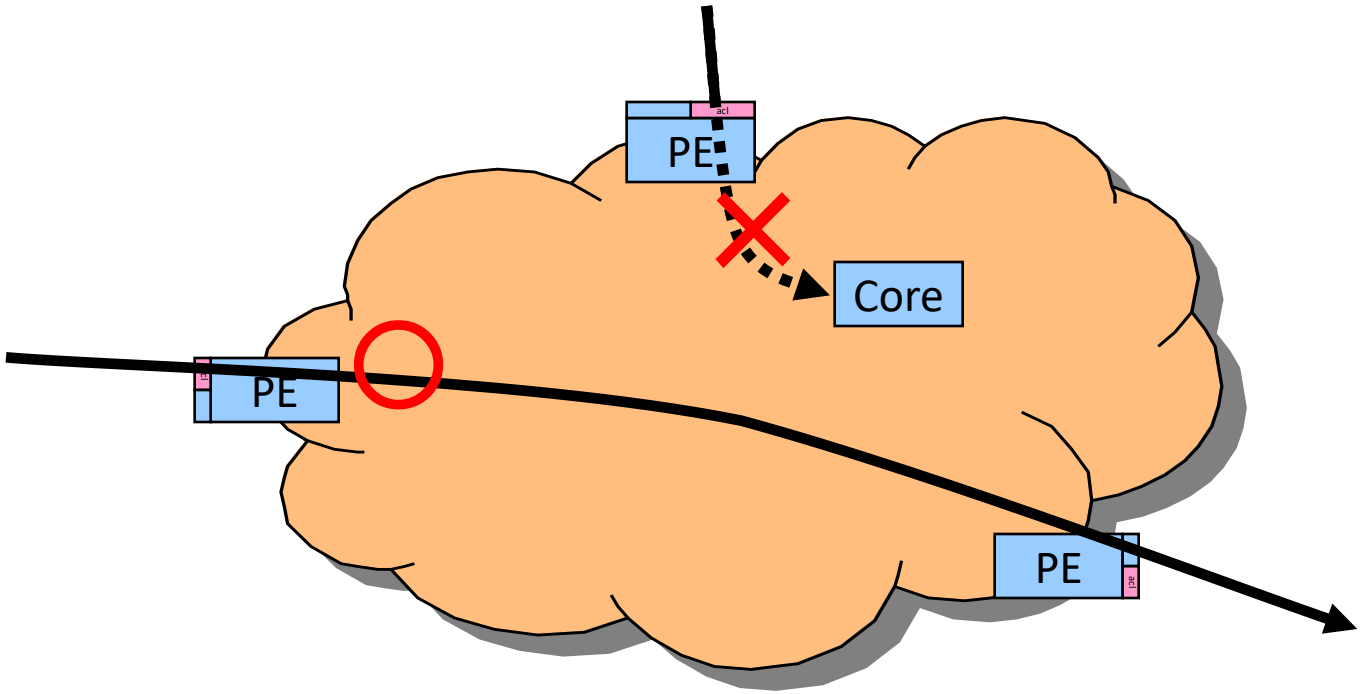


Infrastructure ACL

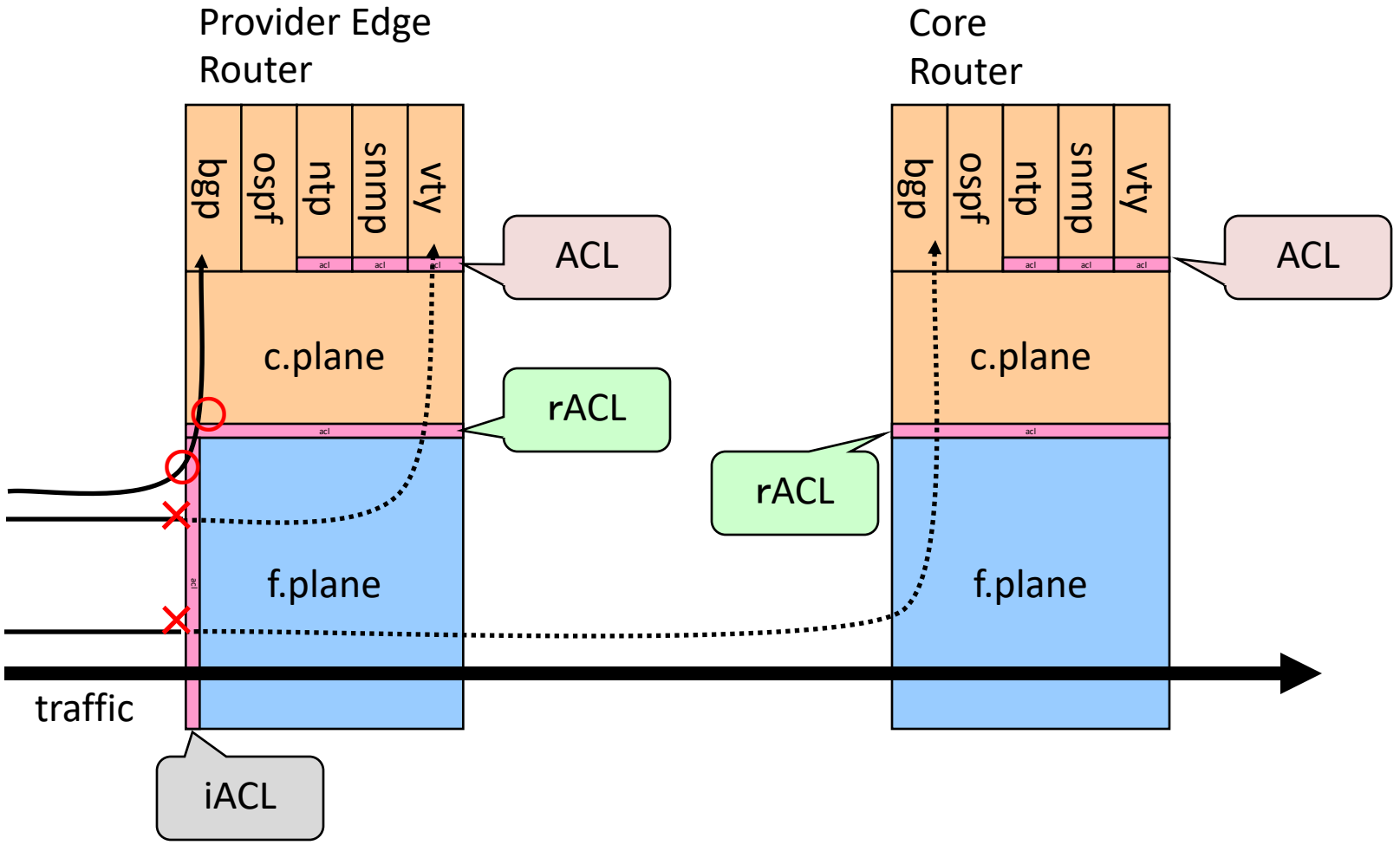
- to protect our management traffic
  - not too much
  - ping, traceroute to our devices should be workable
- deny packets from INFRA and to INFRA on edge
  - INFRA: routers, step hosts and so on
    - these ip range should stay inside

Infrastructure ACL (iACL)

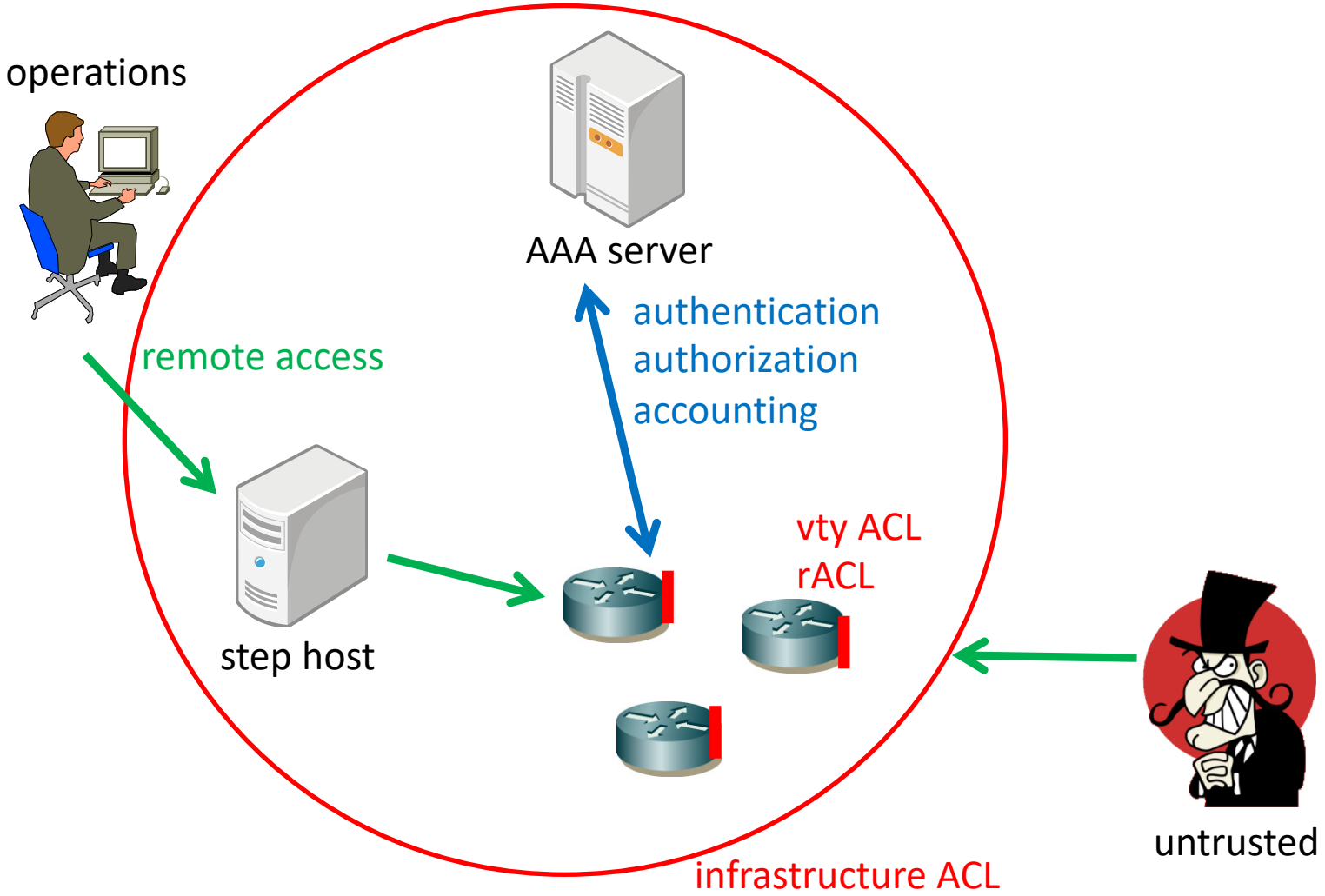
- enforce a policy on the network edge



multiple ACLs to protect Devices



protecting devices



Infrastructure Filters

- Develop list of required protocols that are sourced from outside your AS and access core routers
  - Example: eBGP peering, GRE, IPSec, etc.
  - Use classification filters as required
- Identify core address block(s)
  - This is the protected address space
  - Summarization is critical for simpler and shorter filters

Host security

- Some hosts are located at the boundary of your network
- Providing public services
  - Web, DNS, etc
- They are also be protected
- The idea is similar to the infrastructure devices
  - Accept traffic only from necessary sources

Host security

- Services are normally built on top of general servers
  - Linux, Windows
- They potentially have tons of functions most of which are not used for the specific service
- We must pay attention to the configuration to keep only required services running
  - Configuration update
  - Software update
  - OS upgrade

Hands on

- In this session, we have two hands ons
  - Host firewall hands on (using ufw)
  - Scanning hands on (using nmap)