Campus Network Security: Configuration Details

Campus Network Design & Operations Workshop

UNIVERSITY OF OREGON

Last updated 4th January 2019

NSRC
Network Startup Resource Center

Background

- Too many campus network operators believe that firewall insertion in the upstream segment will solve all their campus security needs
- Today's end-user devices all have built-in firewalls turned on
- Most attacks on today's network infrastructure come from the internal users/devices
- Most viruses and exploits are initiated by users clicking malicious links or opening infected emails
  - Both lead to malicious software being installed

Background

- Firewalls are major bottlenecks in today's high capacity, high speed campus backbones (real or future planned)
- A modern (21st century) approach to network security needs to consider modern approaches, namely:
  - Protect the critical infrastructure assets of the campus
    - Firewalls have a role here
    - As do other strategies
  - Allow users to do their work, their research, and their education

Campus Security Configuration Details

- Presentation explores the securing of the campus network
  - Securing Campus Network Devices
  - Border Router filtering
  - Anti-spoofing filters
  - Routing Security
  - Know your colleagues
- This effort is part of a larger global effort to secure the global Internet infrastructure
  - See https://manrs.org for more information

Securing Campus Network Devices

Securing Campus Network Devices

- Campus devices include:
  - Routers
  - Switches
  - Wireless access points
  - Servers (virtual machines and their hosts)
- All need to have management access secured so that only the campus IT staff can access these device management interfaces
- Device security is implemented in two places:
  - Protecting the control plane
  - Provisioning dedicated management VLANs

Securing Routers

- Restrict access to the console and auxiliary ports
  - Campus routers (core and border) are usually in locked equipment cabinets in the campus core data-centre
  - Datacentre access is restricted to IT staff – physical access security best practices apply here
- Restrict login access over the network
  - Turn off telnet – still enabled by default on many devices
  - Set up SSH (Secure Shell) – version 2 only
  - Protect the device control plane login ports with filters

Router access filter example

- Protect login access to router control plane over the network:
  - Filters to allow access from the Campus NOC address space
  - Filters to allow access from other campus device management interfaces
    - Allows device-to-device connections for troubleshooting
- User authentication, authorisation, accounting:
  - Each user must have an account
  - Use centralised AAA system such as TACACS+ (or Radius)
  - Authorisation allows for different classes of users:
    - Standard – for monitoring users / systems
    - Administrator – to modify configurations

Cisco IOS example

```
aaa new-model
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa authorization commands 0 default group tacacs+ none
aaa accounting commands 15 default start-stop group tacacs+
!
tacacs server CAMPUS
 address ipv4 100.64.0.5
 key C4mpu5K3Y
!
ip access-list extended v4-vty
 permit ip host 100.64.0.0 0.0.0.255 any     ! NOC
 permit ip host 100.64.16.0 0.0.15.255 any   ! Mgmt VLANs
 deny   ip any any log
!
line vty 0 4
 access-class v4-vty in
 transport preferred none
 transport input ssh
 transport output ssh
!
```

Define AAA

tacacs+ server definition

Who gets access to VTYs

Protect the VTYs

NSRC
Network Startup Resource Center

Securing Switches

- Restrict access to the console and auxiliary ports
  - Campus switches (distribution and access) are usually in locked equipment cabinets in strategic parts of buildings
  - Physical access needs to be considered carefully
- Restrict login access over the network
  - Turn off telnet – still enabled by default on many devices
  - Set up SSH (Secure Shell) – version 2 only
  - Protect the control plane login ports with filters on the management VLAN interface

Securing Wireless Access Points

- Restrict access to the console port
  - Many modern APs have no physical console port, instead having just a single ethernet interface
  - Campus wireless access points are usually mounted on ceilings, well out of reach
- Restrict login access over the network
  - Most modern APs are managed by dedicated software or hardware controllers
  - Hardware controllers need to be protected like routers or switches
  - Software controllers running on laptops or tablets need to have proper management access permissions

Securing Servers

- Today's campus servers are:
  - Physical hardware which hosts many virtual machines
  - Virtual machines sitting on host hardware
    - The days of one server occupying one physical hardware platform are past
- Physical Hardware
  - LAN interfaces, with VLANs usually trunked to a Firewall for filtering
  - Management interface, for managing the parent OS
  - IPMI interface, for accessing the BIOS of the physical hardware, for OS installation and basic maintenance

Securing Servers – Physical Hardware

- LAN interfaces for connecting hosted VMs to the campus infrastructure
  - Security: see VM discussion on next slide
- Management interface for management of the parent operating system
  - Security: dedicated management VLAN firewalled from the campus network
- IPMI interface for last resort BIOS access
  - Security: dedicated LAN, isolated from the campus network
  - Or use other out of band access (serial console) rather than IPMI

Securing Servers – VMs

- LAN interface connecting to the outside world
- LAN delivered usually as VLAN trunk via the physical hosting hardware
- Firewalls have an important role protecting these VMs
- Most OSes used on VMs have built-in firewalls – these must also be used
- Filters allow access to the service being hosted only, for example:
  - Webserver filter allows incoming HTTP and HTTPS, and SSH from Campus NOC and content owner for management and update access
  - (in addition to DNS queries made by webserver, ICMP in/out, etc)

Securing Servers

iptables example

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2:240]
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
-A INPUT -p esp -j ACCEPT
-A INPUT -p ah -j ACCEPT
-A INPUT -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -s 192.168.1.0/24 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -s 192.168.1.250/32 -p udp -m udp --dport 161 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

All ICMP

Allow established TCP

NOC SSH access

webserver

NMM SNMP access

Accessing Campus Devices

- Most access to campus devices will be carried out from on-site within the campus NOC
- But what about remote access?
  - Not in the NOC
  - Completely off campus
- Solution: Jumphost
  - Create an SSH server host (this is all it does) within the NOC
  - It listens only on SSH port – has no other services running
  - Connect there, and then SSH onwards to the campus devices
  - (Or a Secure VPN access server)

Border Router Filtering

Border Router Filtering

- The Border Router is the first line of “defence” for the Campus
  - Handles all the routing with the NREN
  - Runs OSPF/IS-IS with the Core Router
  - More advanced Campus networks use BGP with NREN & internal
  - Connects the Science DMZ (if there is one)
  - Implements packet filtering (in and out) as required

Border Router Filtering

- As mentioned in the Campus Security Overview presentation there is minimal need to block incoming ports
- Campuses do need to pay close attention to certain assets, and certain types of services which are only used on campus
- Two examples follow:
  - Simple example, minimal filtering
  - Complex example, needs significant ongoing maintenance
  - 100.64.0.0/16 has been used as the Campus IPv4 address block

Simple Example

- The following example shows a simple border router filter
  - Blocks traffic sourced from private address space
  - Protects the management VLANs of the campus
  - Blocks access to services only used on campus

  - In the examples:
    - 100.64.0.0/22 is used for campus network devices
    - 100.64.254.0/24 is used for Science DMZ
    - 100.64.255.0/24 is used for campus services (eg WWW, SMTP)

Simple Border Filter (Inbound)

```
ip access-list extended CAMPUS-IN
 deny   ip 10.0.0.0 0.255.255.255 any   ! Private address space
 deny   ip 172.16.0.0 0.15.255.255 any  ! Private address space
 deny   ip 192.168.0.0 0.0.255.255 any  ! Private address space
 deny   ip 100.64.0.0 0.0.255.255 any   ! Block our address origin from outside
 deny   tcp any any eq telnet           ! telnet
 deny   udp any any range 135 139       ! netbios
 deny   tcp any any range 135 139       ! netbios
 deny   udp any any eq tftp             ! TFTP
 deny   udp any any eq snmp             ! SNMP
 deny   udp any any eq snmptrap         ! SNMP traps
 deny   udp any any eq 514              ! Syslog
 deny   tcp any any eq 515              ! Printer protocol
 permit icmp any any                    ! Permit all ICMP (indicative)
 permit ip any any                      ! Permit all IP
```

Simple Border Filter (Outbound)

```
ip access-list extended CAMPUS-OUT
 deny   tcp any any eq telnet            ! telnet
 deny   udp any any range 135 139        ! netbios
 deny   tcp any any range 135 139        ! netbios
 deny   udp any any eq tftp              ! TFTP
 deny   udp any any eq snmp              ! SNMP
 deny   udp any any eq snmptrap          ! SNMP traps
 deny   udp any any eq 514               ! Syslog
 permit tcp any host 100.64.0.25 eq 25   ! SMTP only from Campus SMTP relay
 deny   tcp any any eq 25                ! Block all SMTP
 permit icmp 100.64.0.0 0.0.255.255 any ! Permit all ICMP (indicative)
 permit ip 100.64.0.0 0.0.255.255 any    ! Permit all IP
 permit ip host <NREN p-t-p> any         ! Permit P-T-P link to NREN
 deny   ip any any
```

Complex Example

- The following example shows a complex border router filter
  - The filter has included many vulnerabilities from this century (including some which are long solved)
  - Doesn't allow any user to set up a public service on internal infrastructure outside of the Science DMZ
  - Includes all the features of the previous "simple example"
- Note that this example is quite restrictive
  - Contrary to "Campus Networks are Open Networks" advice
  - Included to show detailed filter configuration possibilities

Complex Border Filter (inbound)

```
ip access-list extended CAMPUS-IN
 deny   ip 10.0.0.0 0.255.255.255 any       ! Private address space
 deny   ip 172.16.0.0 0.15.255.255 any      ! Private address space
 deny   ip 192.168.0.0 0.0.255.255 any      ! Private address space
 deny   ip 100.64.0.0 0.0.255.255 any       ! Block our address origin from outside
 permit tcp any any established             ! Allow internal sourced TCP connections
 permit ip  any 100.64.254.0 0.0.0.255      ! Allow all to Campus Science DMZ
 deny   udp any any eq 19                   ! Chargen (Character generator)
 deny   tcp any any eq 19                   ! Chargen (Character generator)
 deny   tcp any any eq telnet               ! telnet
 deny   udp any any range 135 139           ! netbios
 deny   tcp any any range 135 139           ! netbios
 deny   udp any any eq tftp                 ! TFTP
 deny   udp any any eq sunrpc               ! SUN remote proc call
 deny   udp any any eq snmp                 ! SNMP
 deny   udp any any eq snmptrap             ! SNMP traps
 deny   tcp any any eq 445                  ! Blaster worm
 deny   udp any any eq 514                  ! Syslog
...continued...
```

Complex Border Filter (inbound)

```
...
 deny    tcp any any eq 515                    ! Printer protocol
 deny    tcp any any eq 1025                   ! MS 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    udp any any eq 3544                   ! Teredo
 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
 deny    tcp any any eq 20000                  ! SCADA control ports
 deny    udp any any eq 53413                  ! Netcore Router backdoor
...continued...
```

Complex Border Filter (inbound)

```
...
 permit icmp any any                              ! Allow all ICMP
 permit udp any eq isakmp any eq isakmp           ! Allow IPsec VPNs
 permit esp any any                               ! Allow IPsec VPNs
 permit udp any any gt 1023                       ! Allow unprivileged UDP ports
 permit udp any host 100.64.255.10 eq 53          ! Allow to DNS resolvers
 permit udp eq 53 any host 100.64.255.10          ! Allow to DNS resolvers
 permit udp any host 100.64.255.11 eq 53          ! Allow to DNS resolvers
 permit udp eq 53 any host 100.64.255.11          ! Allow to DNS resolvers
 permit udp any eq 123 host 100.64.255.5          ! Allow NTP to NTP host
 permit udp any host 100.64.255.5 eq 123          ! Allow NTP to NTP host
 deny   udp any any                               ! and block all other UDP
 permit tcp any host 100.64.255.15 eq 25          ! Allow to Mail Server
 permit tcp any host 100.64.255.15 eq 443         ! Allow to WebMail
 permit tcp any host 100.64.255.16 eq 80          ! Allow to Campus Website (HTTP)
 permit tcp any host 100.64.255.16 eq 443         ! Allow to Campus Website (HTTPS)
 permit tcp any host 100.64.255.19 eq 443         ! Allow to Student e-Learning
 permit tcp any host 100.64.255.22 eq 22          ! Allow Campus JumpHost
 deny   ip  any any                               ! There should be nothing else
```

Complex Border Filter (outbound)

```
ip access-list extended CAMPUS-OUT
 permit udp host 100.64.255.5 eq 123          ! Allow NTP to NTP host
 permit udp host 100.64.255.5 any eq 123      ! Allow NTP to NTP host
 deny   udp any any eq 123                    ! No one can NTP to the world
 deny   udp any any eq 19                     ! Chargen (Character generator)
 deny   tcp any any eq 19                     ! Chargen (Character generator)
 deny   tcp any any eq telnet                 ! telnet
 deny   udp any any range 135 139             ! netbios
 deny   tcp any any range 135 139             ! netbios
 deny   udp any any eq sunrpc                 ! SUN remote proc call
 deny   tcp any any eq 445                    ! Blaster worm
 deny   tcp any any eq 1025                   ! MS 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
...continued...
```

Complex Border Filter (outbound)

```
deny   tcp any any eq 3128                    ! MyDoom! worm
deny   tcp any any eq 5000                    ! WindowsXP UPnP port
deny   udp any any eq 3544                    ! Teredo
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
deny   tcp any any eq 20000                   ! SCADA control ports
deny   udp any any eq 53413                   ! Netcore Router backdoor
permit icmp 100.64.0.0 0.0.255.255 any        ! Permit all ICMP (indicative)
permit udp host 100.64.255.10 any eq 53       ! DNS only from Campus DNS resolvers
permit udp eq 53 host 100.64.255.10 any       ! DNS only from Campus DNS resolvers
permit udp host 100.64.255.11 any eq 53       ! DNS only from Campus DNS resolvers
permit udp eq 53 host 100.64.255.11 any       ! DNS only from Campus DNS resolvers
permit tcp any host 100.64.255.25 eq 25       ! SMTP only from Campus SMTP relay
deny   tcp any any eq 25                      ! Block all SMTP
permit icmp 100.64.0.0 0.0.255.255 any        ! Permit all ICMP (indicative)
permit ip 100.64.0.0 0.0.255.255 any          ! Permit all IP
permit ip host <NREN p-t-p> any               ! Permit P-T-P link to NREN
deny   ip any any
```

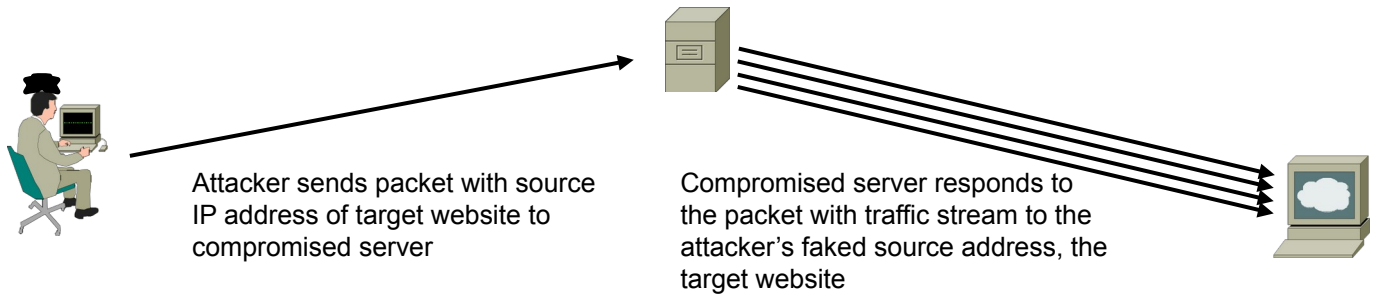
Border Router Filtering

- The previous two examples are just that, examples!
  - Do NOT cut and paste these into any network
- Simple example:
  - Should be sufficient for most campuses – modify to suit
- Complex example:
  - Very restrictive – more Enterprise than Campus style

Anti-Spoofing Filters

Anti-Spoofing Filters

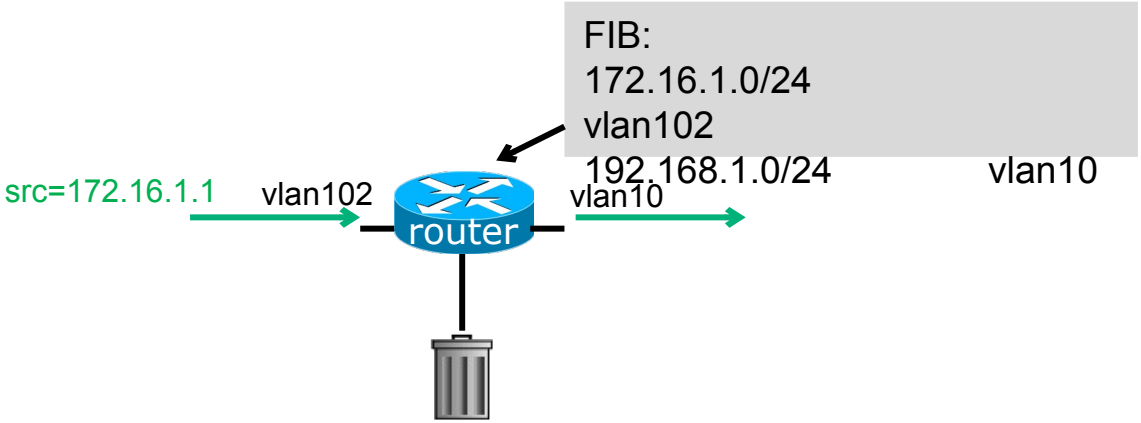
- Devices which have been compromised are well known sources of Distributed Denial of Service (DDoS) attacks
  - The compromised device sends a stream of packets with source IP address of the target for the attack
  - The destination responds to the faked source IP address



Anti-Spoofing Filters

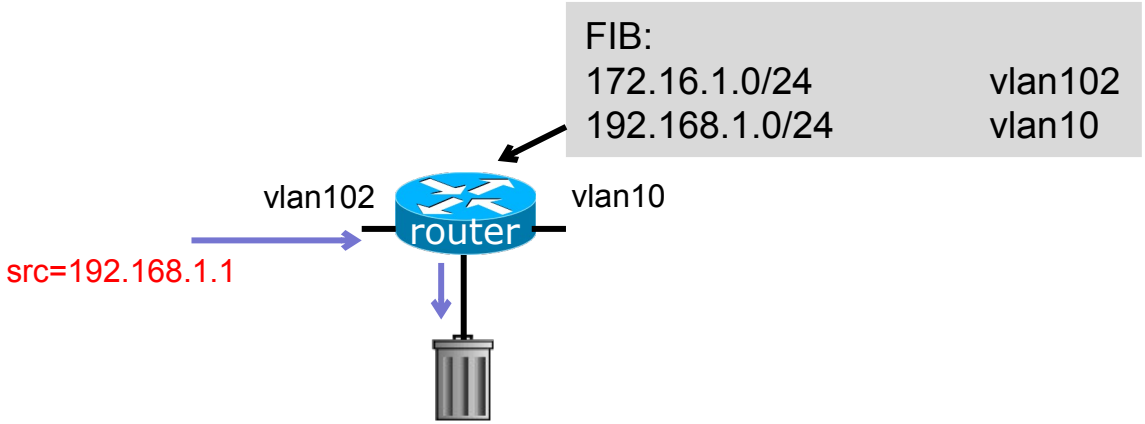
- End devices connected to the Internet must only send IP packets from the IP address assigned to that device
- Best practice today for campus network operators is to block all IP traffic from a VLAN that is not sourced from the IP address range assigned to that VLAN
  - This is done on the campus core router, before any NAT
- The technique used is called “Unicast Reverse Path Forwarding”
  - Simple discard of the spoofed packet by the campus core router hardware

What is uRPF?



- Router compares source address of incoming packet with FIB entry
  - If FIB entry interface matches incoming interface, the packet is forwarded
  - If FIB entry interface does not match incoming interface, the packet is dropped

What is uRPF?



- Router compares source address of incoming packet with FIB entry
  - If FIB entry interface matches incoming interface, the packet is forwarded
  - If FIB entry interface does not match incoming interface, the packet is dropped

Anti-Spoofing Example

- Core router configuration example of anti-spoofing filter using unicast reverse-path forwarding
  - Note: no packet filters needed

```
interface VLAN 101
 description Staff in Building 1
 ip address 100.64.101.1 255.255.255.0
 ip verify unicast reverse-path
 ipv6 address 2001:DB8:1:101::1/64
 ipv6 verify unicast reverse-path
!
interface VLAN 102
 description Student in Building 1
 ip address 100.64.102.1 255.255.255.0
 ip verify unicast reverse-path
 ipv6 address 2001:DB8:1:102::1/64
 ipv6 verify unicast reverse-path
!
...
```

NAT rules

- Check that your NAT only translates *private* address space used internally in your campus, to destinations *outside* your campus
  - A common mistake is to translate any and every source IP address
- Separate NAT pools per subnet or building allow you to track down problems from external reports more easily

Routing Security

Routing Security

- For campuses with their own address space
  - (And maybe also using BGP)
- Route Origin Validation is an important technique towards helping secure the routing system
- Uses Resource Public Key Infrastructure (RPKI) to validate routes
  - Proves that routes are coming from the legitimate holder of the IP address resource

Benefits of RPKI – Routing

- Prevents route hijacking
  - A prefix originated by an AS without authorisation
  - Reason: malicious intent
- Prevents mis-origination
  - A prefix that is mistakenly originated by an AS which does not own it
  - Also route leakage
  - Reason: configuration mistake / fat finger

BGP Security (BGPsec)

- Extension to BGP that provides improved security for BGP routing
- Being worked on by the SIDR Working Group at the IETF
- Implemented via a new optional non-transitive BGP attribute that contains a digital signature
- Two components:
  - BGP Prefix Origin Validation (using RPKI)
  - BGP Path Validation

Route Origin Authorisation (ROA)

- A digital object that contains a list of address prefixes and one AS number
- It is an authority created by a prefix holder to authorise an Autonomous System to originate one or more specific route advertisements
- Publish a ROA using your RIR member portal

Router Origin Validation

- Networks using BGP can check the validation state of received routes
  - Router must support RPKI
  - Checks an RP cache / validator
  - Validation returns 3 states:
    - Valid = when authorization is found for prefix X
    - Invalid = when authorization is found for prefix X but not from ASN Y
    - Unknown = when no authorization data is found

Using RPKI

- NRENs and campuses using BGP can now make decisions based on RPKI state:
  - Invalid – discard the prefix
  - Not found – let it through (maybe low local preference)
  - Valid – let it through (high local preference)
- More and more router vendors support RPKI
  - Point router to the local RPKI cache
    - Server listens on port 43779
    - Cisco IOS example:

```
router bgp 64512
 bgp rpki server tcp 10.0.0.3 port 43779 refresh 60
```

BGP Table (IPv4)

```
RPKI validation codes: V valid, I invalid, N Not found

Network          Metric LocPrf Path
N*>  1.0.4.0/24       0         37100 6939 4637 1221 38803 56203 i
N*>  1.0.5.0/24       0         37100 6939 4637 1221 38803 56203 i
...
V*>  1.9.0.0/16       0         37100 4788 i
N*>  1.10.8.0/24      0         37100 10026 18046 17408 58730 i
N*>  1.10.64.0/24     0         37100 6453 3491 133741 i
...
V*>  1.37.0.0/16      0         37100 4766 4775 i
N*>  1.38.0.0/23      0         37100 6453 1273 55410 38266 i
N*>  1.38.0.0/17      0         37100 6453 1273 55410 38266 {38266} i
...
I*   5.8.240.0/23     0         37100 44217 3178 i
I*   5.8.241.0/24     0         37100 44217 3178 i
I*   5.8.242.0/23     0         37100 44217 3178 i
I*   5.8.244.0/23     0         37100 44217 3178 i
...
```

RPKI Summary

- All AS operators must consider deploying
  - Which means: **Signing ROAs & dropping invalids**
- Origin validation is important step to securing the routing system
- Doesn't secure the path, but that's next!
- With origin validation, the opportunities for malicious or accidental mis-origination disappear
- FAQ: https://nlnetlabs.nl/projects/rpki/faq/
- MANRS: https://manrs.org

Know your Colleagues

Know your Colleagues

- What happens when there is a network incident affecting your campus connectivity to the NREN and the rest of the Internet?
  - Who do you call?
- Knowing your colleagues at the NREN (and ISP if you connect there too), as well as in other campuses, is extremely useful for helping diagnose and mitigate network incidents, especially DoS attacks on the campus infrastructure
  - Mobile phone numbers, mobile messaging tools (e.g. WhatsApp)
  - Bypasses “customer support” and speeds resolving of serious outages

Resources

- Lots of resources on the Internet
  - www.manrs.org – Mutually Agreed Norms for Routing Security: filtering, routing security, route validation, global coordination
    - MANRS is an initiative of the Internet Society (www.isoc.org)
  - www.sans.org – subscribe to the SANS newsletter
  - www.team-cymru.org/templates.html – a great set of templates for secure configuration of routers and some services
  - www.cert.org – a good resource for lists of vulnerabilities

Mutually Agreed Norms for Routing Security

MANRS Hits Major Milestone with more than 100 Network Operators

The Internet Society announced on 4 December 2018 that the number of network operators that have agreed to Mutually Agreed Norms for Routing Security (MANRS) has surpassed 100, with each participating operator representing dozens, hundreds or even thousands of autonomous system numbers (ASNs).

MANRS

How can MANRS help?

MANRS outlines four simple but concrete actions that network operators should take:

- **Filtering** – Ensure the correctness of your own announcements and of announcements from your customers to adjacent networks with prefix and AS-path granularity
- **Anti-spoofing** – Enable source address validation for at least single-homed stub customer networks, your own end-users, and infrastructure
- **Coordination** – Maintain globally accessible up-to-date contact information
- **Global Validation** – Publish your data, so others can validate routing information on a global scale

A separate set of Actions applies explicitly to Internet Exchange Points.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Questions/Discussion?