

Network Infrastructure Filtering at the border

PacNOG19

28th November - 2nd December 2016

Nadi, Fiji

What we have in network?

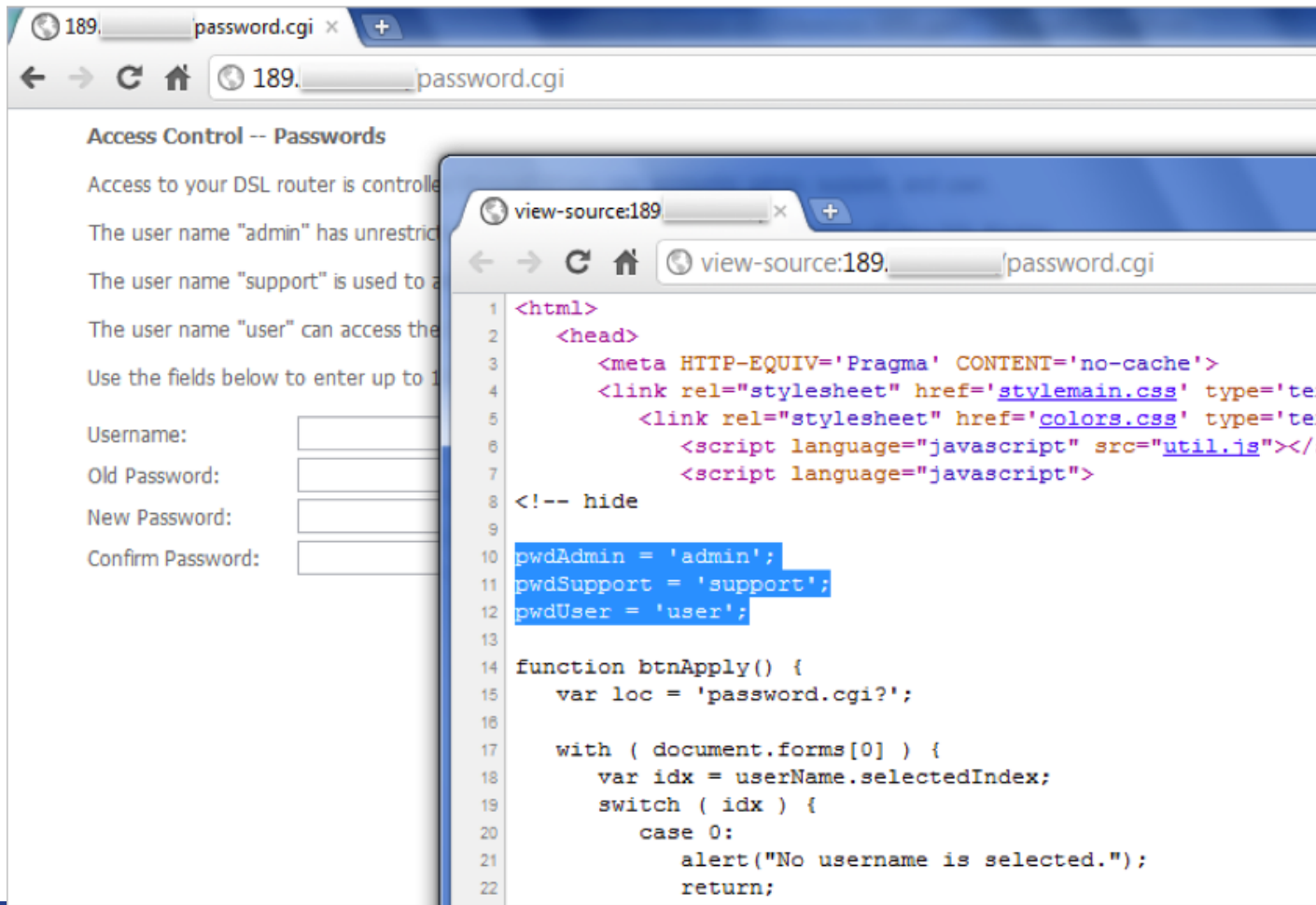
- Router
- Switch
- CPE (ADSL Router / WiFi Router)
- Servers
- PC/Laptop
- Smart Phone

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



The image shows a web browser window with the address bar displaying '189. password.cgi'. The page title is 'Access Control -- Passwords'. The content explains that access to the DSL router is controlled by passwords and lists the permissions for 'admin', 'support', and 'user' users. Below this, there are input fields for 'Username:', 'Old Password:', 'New Password:', and 'Confirm Password:'. A second browser window, titled 'view-source:189. password.cgi', is overlaid on the first, showing the source code of the page. The source code is an HTML document with a head section containing meta and link tags, and a body section with a hidden script block. The script block contains three variables: 'pwdAdmin = 'admin'', 'pwdSupport = 'support'', and 'pwdUser = 'user''. Below these variables is a function 'btnApply()' which sets a location variable 'loc' to 'password.cgi?', iterates over the form elements, and alerts the user if no username is selected.

Access Control -- Passwords

Access to your DSL router is controlled by passwords.

The user name "admin" has unrestricted access to the router.

The user name "support" is used to access the router for support.

The user name "user" can access the router for basic configuration.

Use the fields below to enter up to 16 characters for the password.

Username:

Old Password:

New Password:

Confirm Password:

```
1 <html>
2   <head>
3     <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
4     <link rel="stylesheet" href='stylemain.css' type='text/css'>
5     <link rel="stylesheet" href='colors.css' type='text/css'>
6     <script language="javascript" src="util.js"></script>
7     <script language="javascript">
8   <!-- hide
9
10  pwdAdmin = 'admin';
11  pwdSupport = 'support';
12  pwdUser = 'user';
13
14  function btnApply() {
15    var loc = 'password.cgi?';
16
17    with ( document.forms[0] ) {
18      var idx = userName.selectedIndex;
19      switch ( idx ) {
20        case 0:
21          alert("No username is selected.");
22          return;
```

Magnitude of Problem

- 4.5 Million CPEs (ADSL Modems) using a unique malicious DNS
- In early 2012 more than 300,000 CPEs still infected
- 40 malicious DNS servers found

Allow remote access

NETGEAR
SMARTWIZARD

router manager

Wireless-G Router model WGR614v9



Setup

- Basic Settings
- Wireless Settings
- Content Filtering
- Logs
- Block Sites
- Block Services
- Schedule

Maintenance

- Router Status
- Attached Devices
- Backup Settings
- Set Password

Advanced

- Wireless Settings
- Wireless Repeating Function
- Port Forwarding / Port Triggering
- WAN Setup
- LAN Setup

Remote Management

☒ Turn Remote Management On

Remote Management Address:

http://1 . 80

Allow Remote Access By:

☐ Only This Computer:

. . . .

☐ IP Address Range :

From

To

☒ Everyone

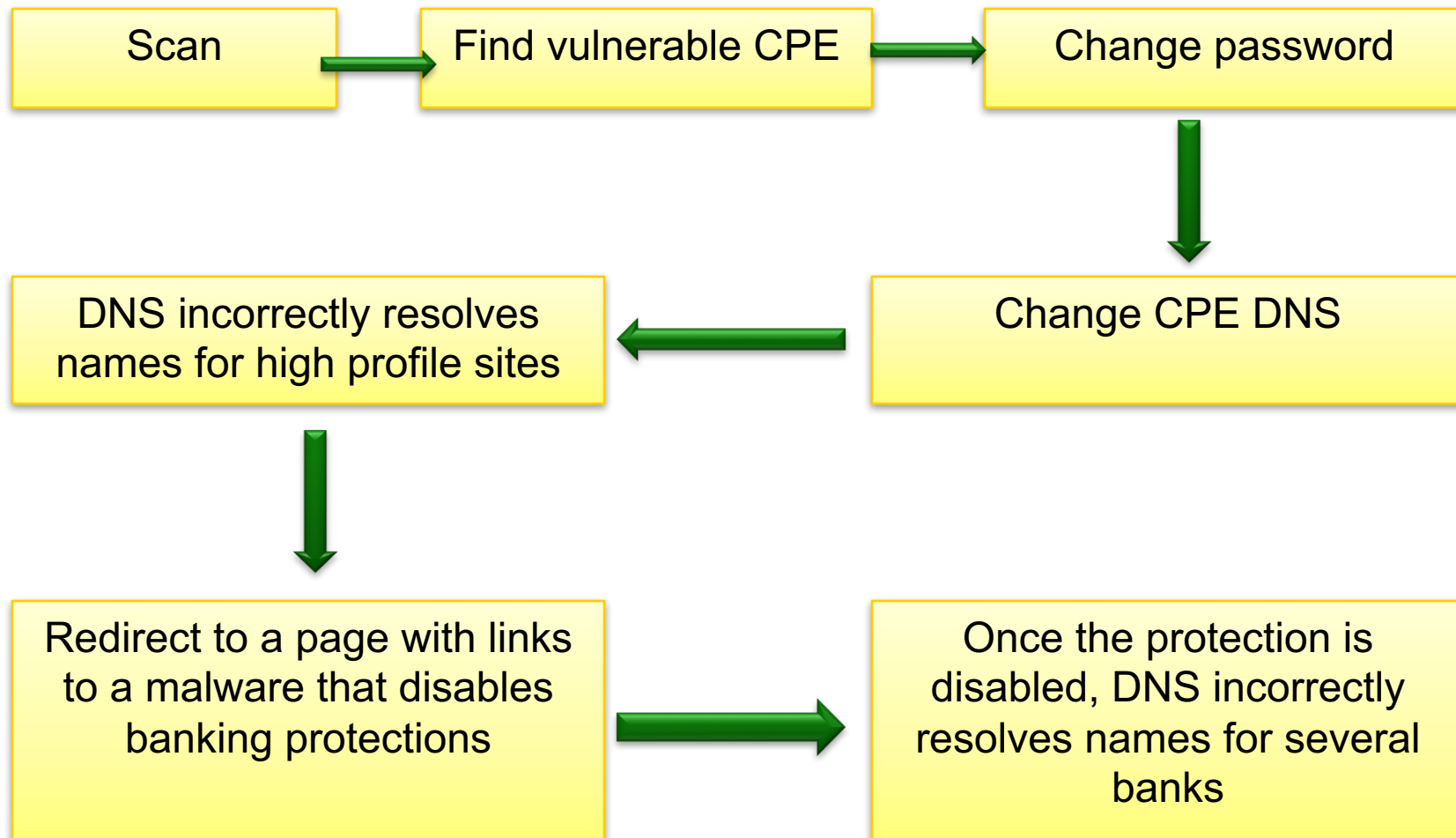
Port Number:

8080

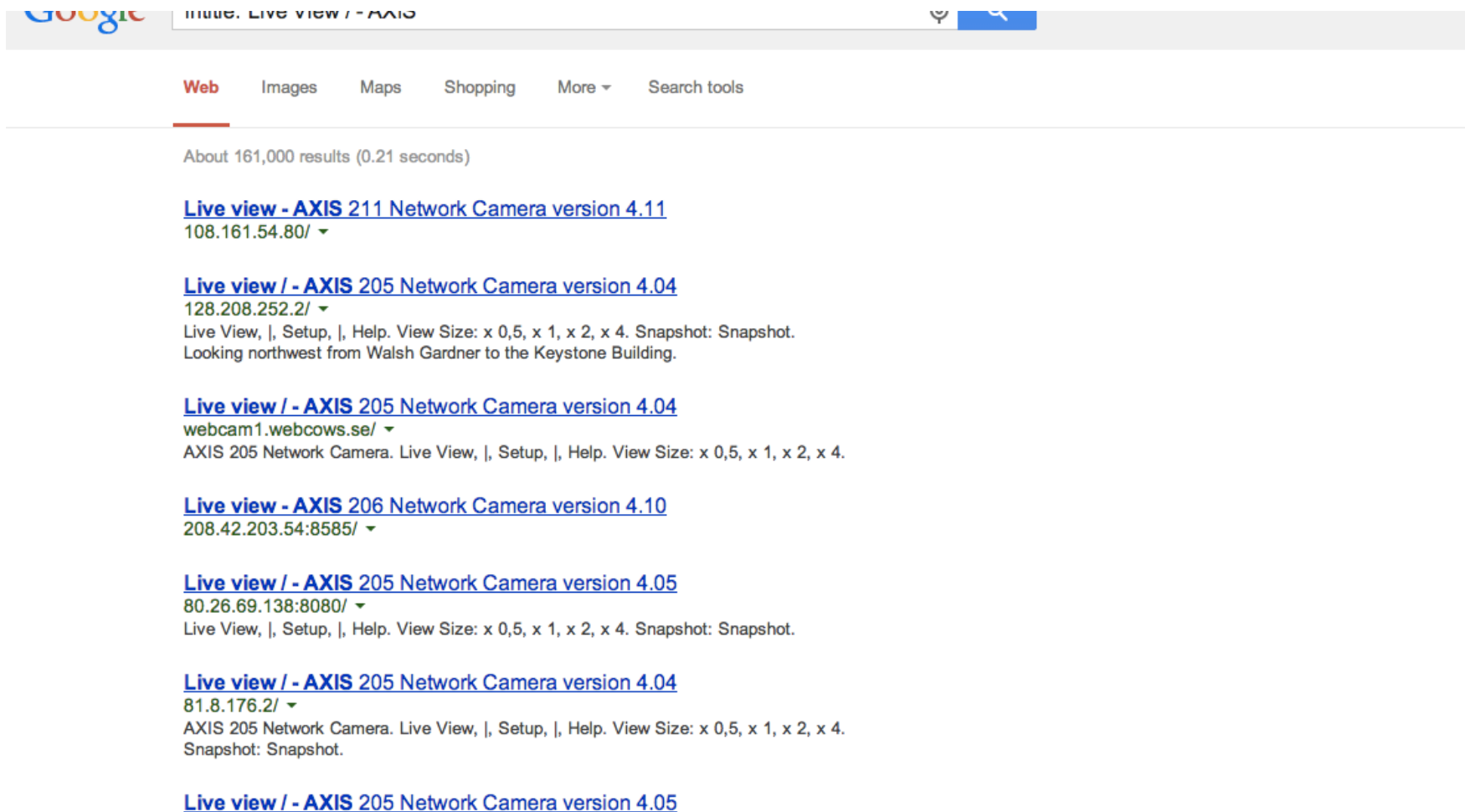
Apply

Cancel



Implication of CPEs Exploited



Finding out open IPcam!!!



The screenshot shows a Google search interface with the query "Live view - AXIS". The search results are filtered to the "Web" tab. The results list several live video feeds from AXIS network cameras. Each result includes a link to the live view, the camera model and version, and the IP address. Some results also provide additional details like view size and snapshot options.

Google  

Web Images Maps Shopping More ▾ Search tools

About 161,000 results (0.21 seconds)

[Live view - AXIS 211 Network Camera version 4.11](#)
108.161.54.80/ ▾

[Live view / - AXIS 205 Network Camera version 4.04](#)
128.208.252.2/ ▾
Live View, |, Setup, |, Help. View Size: x 0,5, x 1, x 2, x 4. Snapshot: Snapshot.
Looking northwest from Walsh Gardner to the Keystone Building.

[Live view / - AXIS 205 Network Camera version 4.04](#)
webcam1.webcows.se/ ▾
AXIS 205 Network Camera. Live View, |, Setup, |, Help. View Size: x 0,5, x 1, x 2, x 4.

[Live view - AXIS 206 Network Camera version 4.10](#)
208.42.203.54:8585/ ▾

[Live view / - AXIS 205 Network Camera version 4.05](#)
80.26.69.138:8080/ ▾
Live View, |, Setup, |, Help. View Size: x 0,5, x 1, x 2, x 4. Snapshot: Snapshot.

[Live view / - AXIS 205 Network Camera version 4.04](#)
81.8.176.2/ ▾
AXIS 205 Network Camera. Live View, |, Setup, |, Help. View Size: x 0,5, x 1, x 2, x 4.
Snapshot: Snapshot.

[Live view / - AXIS 205 Network Camera version 4.05](#)

And more.....

IOActive Lights Up Vulnerabilities for Over Half a Million Belkin WeMo Users

Popular home automation devices are wide open to attackers

Seattle, US — February 18, 2014 — **IOActive, Inc.**, the leading global provider of specialist information security services, announced today that it has uncovered multiple vulnerabilities in Belkin WeMo Home Automation devices that could affect over half a million^[1] users. Belkin's WeMo uses Wi-Fi and the mobile Internet to control home electronics anywhere in the world directly from the user's smartphone.

Mike Davis, IOActive's principal research scientist, uncovered multiple vulnerabilities in the WeMo product set that gives attackers the ability to:

- Remotely control WeMo Home Automation attached devices over the Internet
- Perform malicious firmware updates
- Remotely monitor the devices (in some cases)
- Access an internal home network

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
- Make sure the most vulnerable devices are in that locked room
- Keep intruders from opening the case
- Protect the portables
- Pack up the backups
- Disable the drives
- 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.

Securing SNMP

```
access-list 99 permit 192.168.1.250
```

```
access-list 99 permit 192.168.1.240
```

```
snmp-server community N3T-manag3m3nt ro 99
```

Securing SSH

```
ipv6 access-list AUTHORIZED_IPV6_HOST
  permit ipv6 host 2405:7600:0:6::250 any
  deny ipv6 any any log
!
ip access-list extended AUTHORIZED_IPV4_HOST
  permit tcp host 103.21.75.5 any eq 22
  deny    tcp any any log
!
line vty 0 4
  access-class AUTHORIZED_IPV4_HOST in
  ipv6 access-class AUTHORIZED_IPV6_HOST in
```


Secure Access with Passwords and Logout Timers

```
line console 0
  login
  password console-pw
  exec-timeout 1 30
!
line vty 0 4
  login
  password vty-pw
  exec-timeout 5 00
!
enable secret enable-secret
username bob secret bob-secret
```

Never Leave Passwords in Clear-Text

- ***service password-encryption*** command
- ~~***password*** command~~
 - Will encrypt all passwords on the Cisco IOS with Cisco-defined encryption type “7”
 - Use “*command password 7 <password>*” for cut/paste operations
 - Cisco proprietary encryption method
- ***secret*** command
 - Uses MD5 to produce a one-way hash
 - Cannot be decrypted
 - Use “*command secret 5 <password>*” to cut/paste another “enable secret” password

Authenticate Individual Users

```
username mike secret mike-secret
```

```
username john secret john-secret
```

```
username chris secret chris-secret
```

```
!
```

```
username staff secret group-secret
```

Radius Authentication (AAA)

```
aaa new-model
```

```
!
```

```
aaa authentication login default group radius  
local
```

```
aaa authorization exec default group radius  
local
```

```
!
```

```
radius-server host 192.168.1.250 auth-port  
1812 acct-port 1813
```

```
radius-server key 7 0130310759262E000B69560F
```

Restrict Access To Trusted Hosts

- Use filters to specifically permit hosts to access an infrastructure device
- Example

```
access-list 103 permit tcp host 192.168.200.7  
    192.168.1.0 0.0.0.255 eq 22 log-input  
access-list 103 permit tcp host 192.168.200.8  
    192.168.1.0 0.0.0.255 eq 22 log-input  
access-list 103 permit tcp host 192.168.100.6  
    192.168.1.0 0.0.0.255 eq 23 log-input  
access-list 103 deny ip any any log-input  
!  
line vty 0 4  
access-class 103 in  
transport input ssh
```

1. SSH to NOC

2. Telnet to router

Syslog, TFTP, AAA, DNS, SMTP

NetFlow, SNMP

NOC

Banner – What Is Wrong ?

```
banner login ^C
```

```
You should not be on this device.
```

```
Please Get Off My Router!!
```

```
^C
```

More Appropriate Banner

!!!! WARNING !!!!

You have accessed a restricted device.

All access is being logged and any
unauthorized access will be prosecuted to the
full extent of the law.

Centralized Log (syslog)

```
Router(config)# logging 192.168.0.30
```

```
Router(config)# logging trap 3
```

```
Router(config)# logging facility local3
```

Trap:

Emergency: 0
Alert: 1
Critical: 2
Error: 3
Warning: 4
Notice: 5
Informational: 6
Debug: 7

Facility:

local0
Local1
Local2
Local3
Local4
Local5
Local6
and local7

Configuration change logging

```
Router# configure terminal
```

```
Router(config)# archive
```

```
Router(config-archive)# log config
```

```
Router(config-archive-log-config)# logging enable
```

```
Router(config-archive-log-config)# logging size 200
```

```
Router(config-archive-log-config)# hidekeys
```

```
Router(config-archive-log-config)# notify syslog
```

```
768962: Feb  1 20:59:45.081 UTC: %PARSER-5-CFGLOG_LOGGEDCMD: User:fakrul logged  
command:!exec: enable
```

```
768963: Feb  1 21:03:17.160 UTC: %PARSER-5-CFGLOG_LOGGEDCMD: User:fakrul logged  
command:no ipv6 prefix-list dhakacom_AS23956_IN_IPv6 description
```

```
768965: Feb  1 21:03:19.182 UTC: %SYS-5-CONFIG_I: Configured from console by fakrul on vty0  
(2405:7600:0:6::250)
```

Turn Off Unused Services

Feature	Description	Default	Recommendation	Command
CDP	Proprietary layer 2 protocol between Cisco devices	Enabled		no cdp run
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
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

Turn Off Unused Services

Feature	Description	Default	Recommendation	Command
PAD Service	Router will support X.25 packet assembler service	Enabled	Disable if not explicitly needed	<code>no service pad</code>
IP source routing	Feature that allows a packet to specify its own route	Enabled	Can be helpful in attacks, disable it	<code>no ip source-route</code>
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	<code>no ip proxy-arp</code>
IP directed broadcast	Packets can identify a target LAN for broadcasts	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it	<code>no ip directed-broadcast</code>

Configuration (Templates)

!configure timezone

service timestamps debug uptime

service timestamps log datetime localtime

service password-encryption

clock timezone UTC +6

! turn off unnecessary services (global)

no ip domain-lookup

no cdp run

no ip http server

no ip source-route

no service finger

no ip bootp server

no service udp-small-servers

! turn off unnecessary services (interface)

Interface GigabitEthernet0/0

no ip redirects

no ip directed-broadcast

no ip proxy arp

no cdp enable

! turn on logging and snmp

logging 192.168.253.56

snmp-server communityTxo~QbW3XM ro
98

!

access-list 99 permit 192.168.253.0
0.0.0.255

access-list 99 deny any log

access-list 98 permit host 192.168.253.51

access-list 98 deny any log

!

Configuration (Templates)

```
line vty 0 4
```

```
access-class 99 in
```

```
exec-timeout 2 0
```

```
transport input ssh
```

```
!
```

```
line con 0
```

```
access-class 99 in
```

```
exec-timeout 2 0
```

```
!
```

```
banner motd #
```

```
!!!! WARNING !!!!
```

```
You have accessed a restricted device.
```

```
!Turn on NTP
```

```
ntp authenticate
```

```
ntp authentication-key 1 md5 -  
UN&/6[oh6
```

```
ntp trusted-key 1
```

```
ntp access-group peer 96
```

```
ntp server 192.168.254.57 key 1
```

```
access-list 96 permit host  
192.168.254.57
```

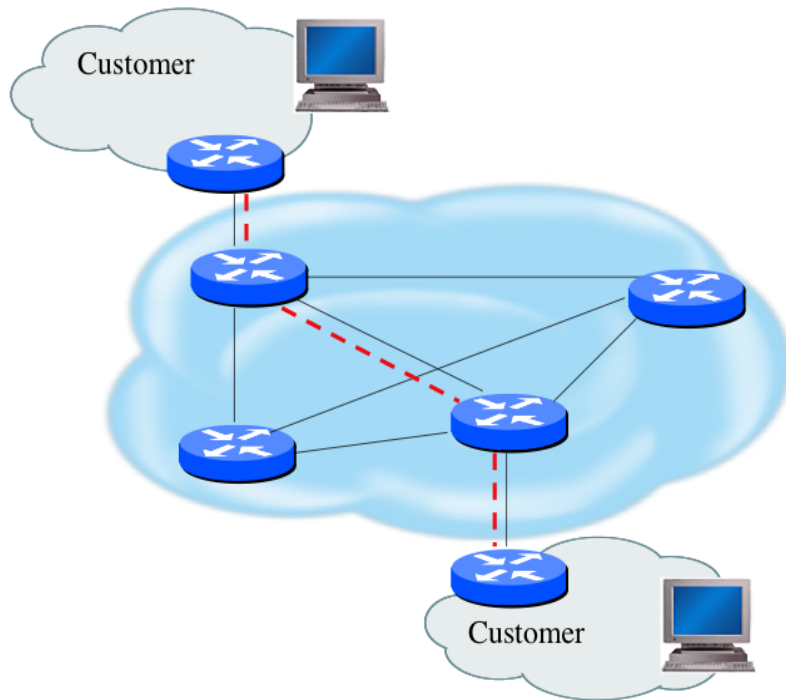
```
access-list 96 deny any log
```

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

DoS Filtering

(* these networks were reallocated and are actually used)

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
Net Test	192.0.2.0 /24
Testing devices *	192.18.0.0 /15
IPv6 to IPv4 relay *	192.88.99.0 /24
RFC 1918 nameservers *	192.175.48.0 /24
End-node auto configuration *	169.254.0.0 /16

Example Incoming IPv4 Bogon Packet Filter

```
ip access-list extended DSL-Incoming
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 169.254.0.0 0.0.255.255 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 224.0.0.0 15.255.255.255 any log
permit icmp any any ttl-exceeded
permit icmp any any echo-reply
permit icmp any any echo
permit tcp any any eq 22 log
permit udp host <ip address> eq domain <subnet range>
permit udp host <ip address> eq domain <subnet range>
permit udp host <ip address> <subnet range> eq ntp
permit udp host <ip address> <subnet range> eq ntp
permit tcp any <my sybnet> established
deny ip any any log
```


Example Incoming IPv4 Bogon Packet Filter

- Bogon and fullbogon peering use different ASNs
- Advertise all fullbogons (IPv4 and IPv6) over a single BGP peering session
- For details: <http://www.team-cymru.org/Services/Bogons/bgp.html>

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 BCP 38

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

Example Outgoing 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 serial 1/1/1.3
```

```
    Description Link to XYZ
```

```
    ip access-group 121 in
```

Infrastructure Filters

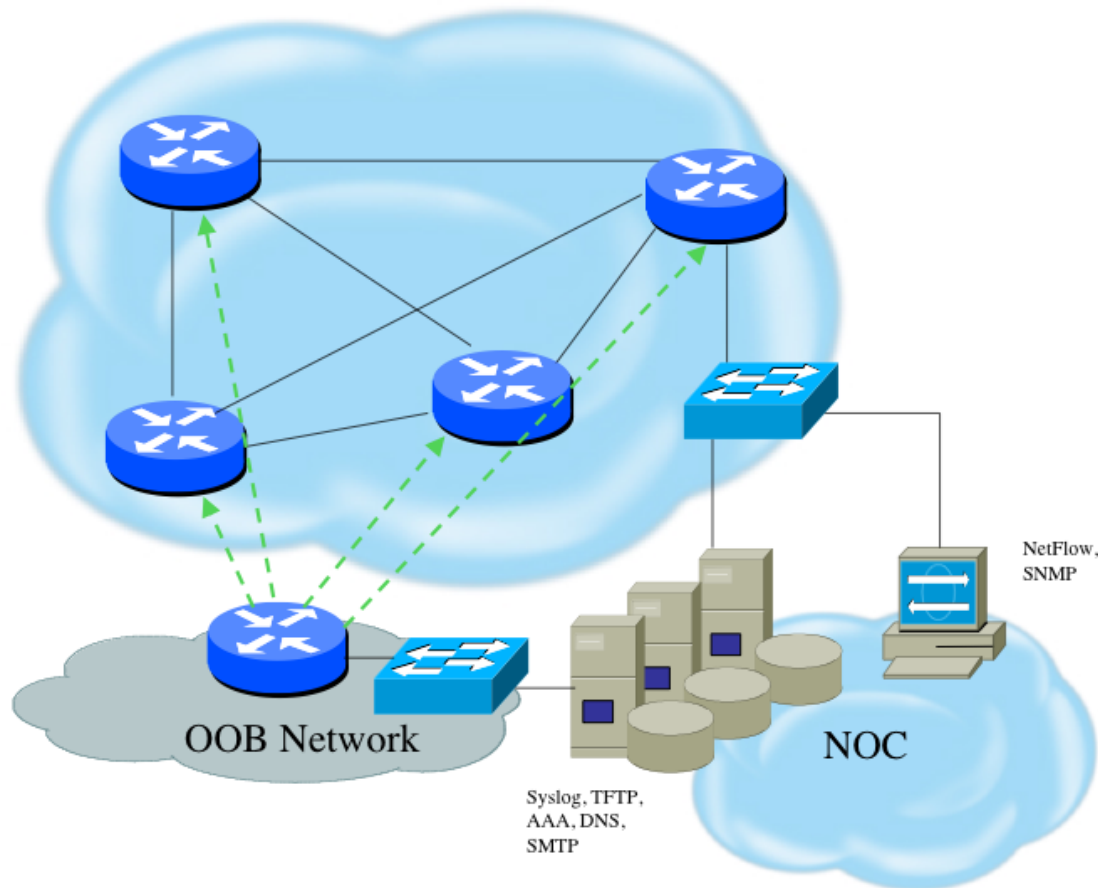
- Permit only required protocols and deny ALL others to infrastructure space
 - Filters now need to be IPv4 and IPv6!
 - Applied inbound on ingress interfaces
- Basic premise: filter traffic destined TO your core routers
- Develop list of required protocols that are sourced from outside your AS and access 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

References

- Articles, documents and templates from Team CYMRU
<http://www.team-cymru.org/ReadingRoom/>
- Google for the information specifics from the vendors you use: “<vendor> security template”

Configuration and Archiving

Device OOB Management



- Out-of-band device management should be used to ensure DoS attacks do not hinder getting access to critical infrastructure devices
- Dial-back encrypted modems are sometimes still used as backup

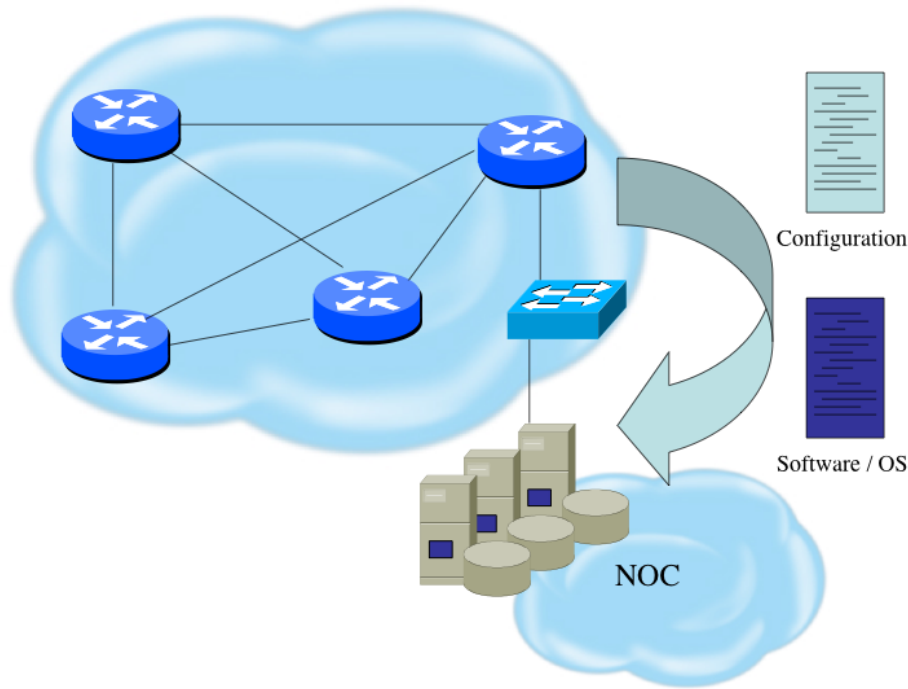
Device Management Common Practice

- SSH primarily used; Telnet only from jumphosts
- HTTP access explicitly disabled
- All access authenticated
 - Varying password mechanisms
 - AAA usually used
 - Different servers for in-band vs OOB
 - Different servers for device authentication vs other
 - Static username pw or one-time pw
 - Single local database entry for backup
- Each individual has specific authorization
- Strict access control via filtering
- Access is audited with triggered pager/email notifications
- SNMP is read-only
 - Restricted to specific hosts
 - View restricted if capability exists
 - Community strings updated every 30-90 days

System Images and Configuration Files

- Careful of sending configurations where people can snoop the wire
 - CRC or MD5 validation
 - Sanitize configuration files
- SCP should be used to copy files
 - TFTP and FTP should be avoided
- Use tools like 'rancid' to periodically check them against modified configuration files

Software and Configuration Upgrade / Integrity



- Files stored on specific systems with limited access
- All access to these systems are authenticated and audited
- SCP is used where possible; FTP is NEVER used; TFTP still used
- Configuration files are polled and compared on an hourly basis (RANCID)
- Filters limit uploading / downloading of files to specific systems
- Many system binaries use MD-5 checks for integrity
- Configuration files are stored with obfuscated passwords