NSRC
Network Startup Resource Center

Internet Infrastructure Security Technology Details

Merike Kaeo
merike@doubleshotsecurity.com

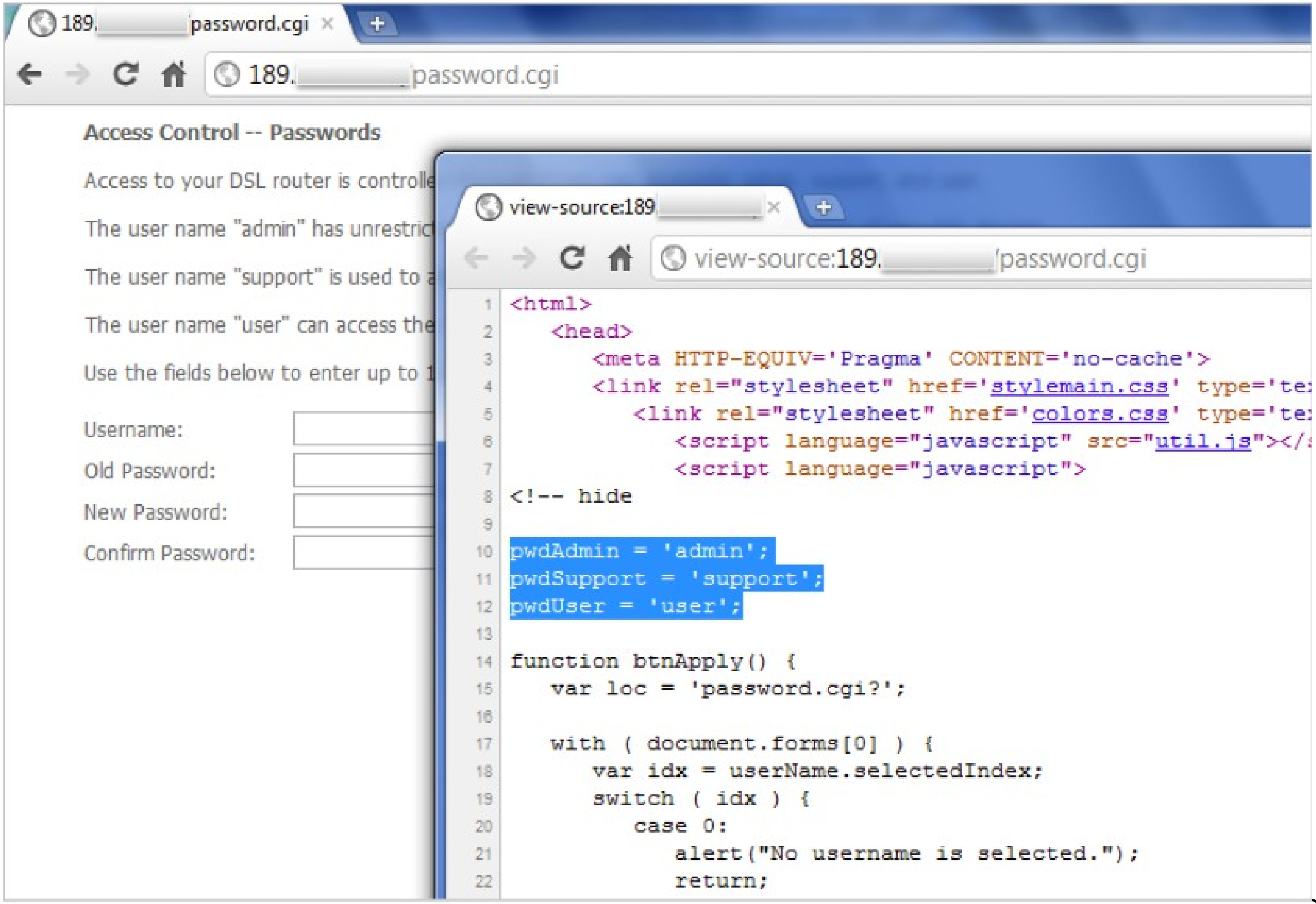
DOUBLE SHOT SECURITY

Securing The Device

Think of ALL Devices

- The following problem was reported last year 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



189.[redacted]password.cgi

189.[redacted]password.cgi

Access Control -- Passwords

Access to your DSL router is controlle

The user name "admin" has unrestric

The user name "support" is used to a

The user name "user" can access the

Use the fields below to enter up to 1

Username:

Old Password:

New Password:

Confirm Password:

view-source:189[redacted]

view-source:189.[redacted]password.cgi

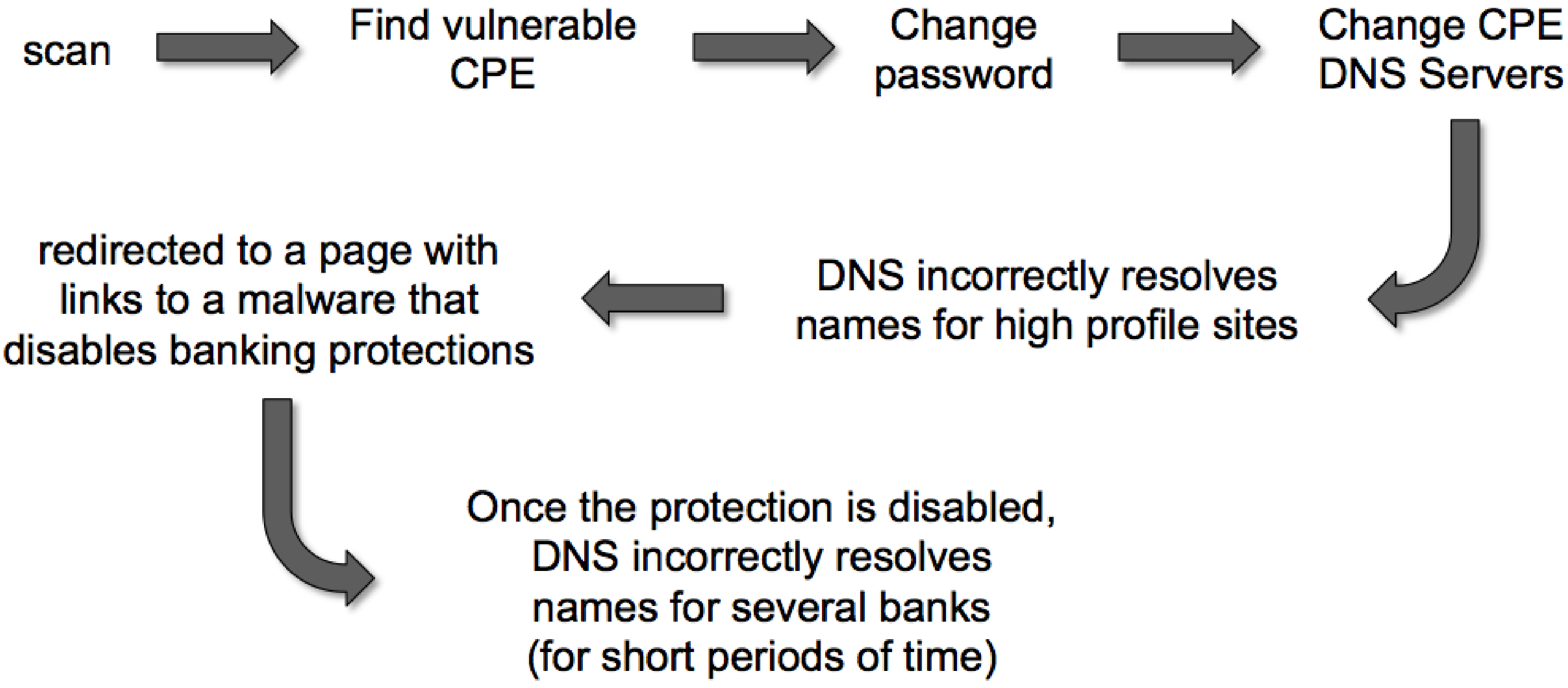
```
<html>
   <head>
      <meta HTTP-EQUIV='Pragma' CONTENT='no-cache'>
      <link rel="stylesheet" href='stylemain.css' type='te:
         <link rel="stylesheet" href='colors.css' type='te:
            <script language="javascript" src="util.js"></:
            <script language="javascript">
<!-- hide

pwdAdmin = 'admin';
pwdSupport = 'support';
pwdUser = 'user';

function btnApply() {
   var loc = 'password.cgi?';

   with ( document.forms[0] ) {
      var idx = userName.selectedIndex;
      switch ( idx ) {
         case 0:
            alert("No username is selected.");
            return;
```

How CPEs Exploited



scan

Find vulnerable CPE

Change password

Change CPE DNS Servers

DNS incorrectly resolves names for high profile sites

redirected to a page with links to a malware that disables banking protections

Once the protection is disabled, DNS incorrectly resolves names for several banks (for short periods of time)

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

Could device hardening have made a difference?

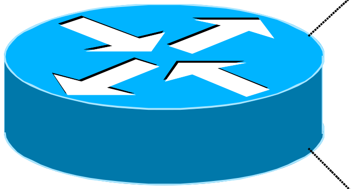
Device Physical Access

- Equipment kept in highly restrictive environments
- Console access
  - password protected
  - access via OOB management
  - configure timeouts
- Individual users authenticated
- Social engineering training and awareness

Device Access Control

- 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

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 merike secret merike-secret
```

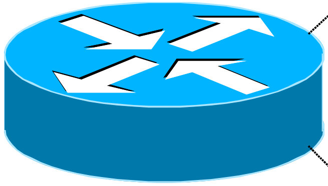
Never Leave Passwords in Clear-Text

- ***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

Management Plane Filters

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

Authenticate Individual Users



username merike secret *merike-secret*

username gaurab secret *gaurab-secret*

username pfs secret *pfs-secret*

~~username staff secret *group-secret*~~

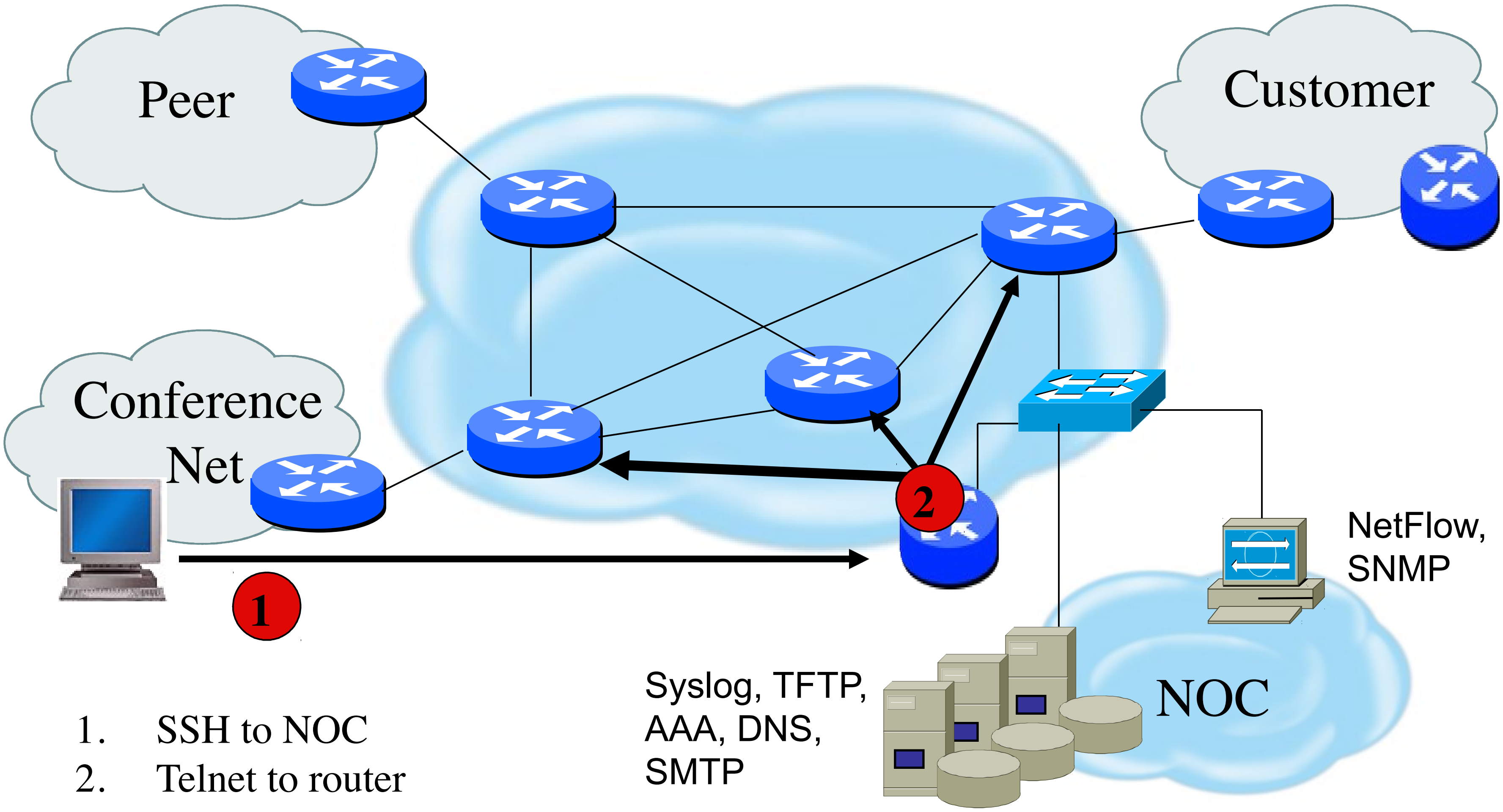
Do NOT have group passwords!

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 telnet
```

Telnet using SSH 'Jumphost'



1. SSH to NOC
2. Telnet to router

Secure SNMP Access

- SNMP is primary source of intelligence on a target network!
- Block SNMP from the outside

```
access-list 101 deny udp any any eq snmp
```

- If the router has SNMP, protect it!

```
snmp-server community fO0bAr RO 8
access-list 8 permit 127.1.3.5
```

- Explicitly direct SNMP traffic to an authorized management station.

```
snmp-server host fO0bAr 127.1.3.5
```

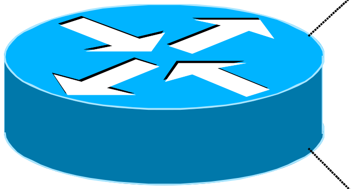
SNMP Best Practices

- Do not enable read/write access unless really necessary
- Choose community strings that are difficult to guess
- Limit SNMP access to specific IP addresses
- Limit SNMP output with views

Secure Logging Infrastructure

- Log enough information to be useful but not overwhelming.
- Create backup plan for keeping track of logging information should the syslog server be unavailable
- Remove private information from logs
- How accurate are your timestamps?

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.

Turn Off Unused Services

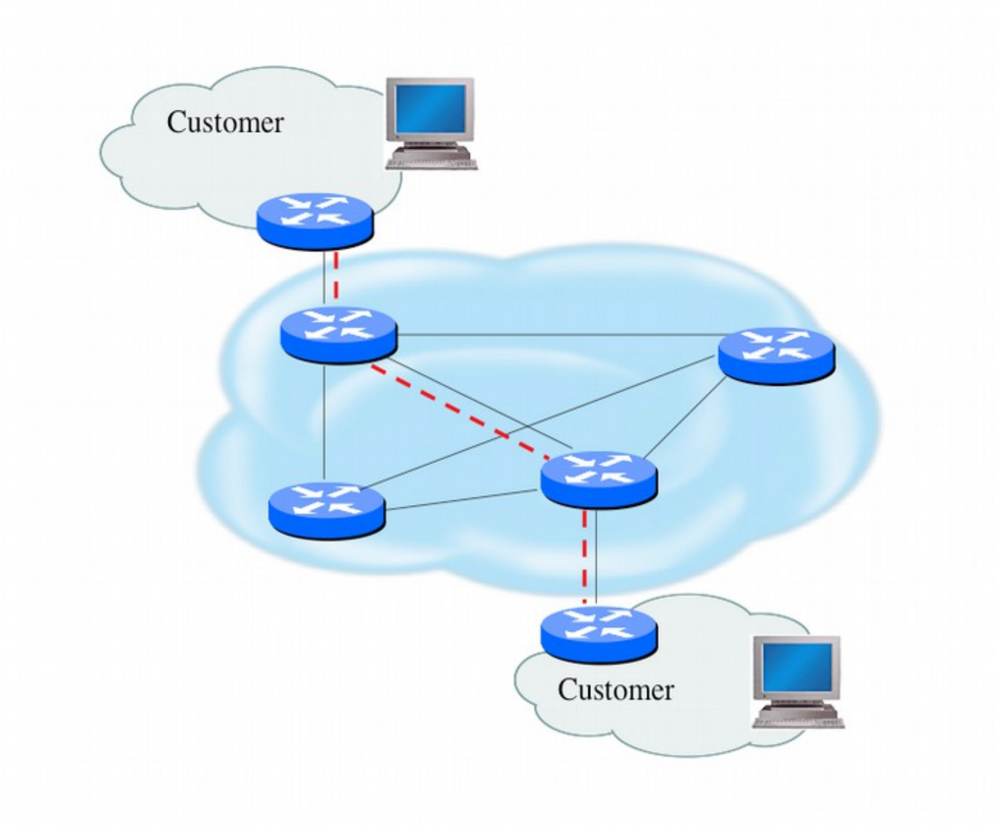
- Global Services
  - no service finger (before 12.0)
  - no ip finger
  - no service pad
  - no service udp-small-servers
  - no service tcp-small-servers
  - no ip bootp server
  - no cdp run
- Interface Services
  - no ip redirects
  - no ip directed-broadcast
  - no ip proxy arp
  - no cdp enable

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

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)

RFC2827 (BCP38) – Ingress Filtering

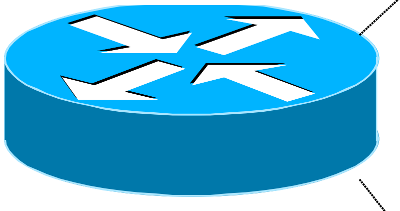
If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.

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.

But What About Egress Filtering?

- In theory, certain addresses should not be seen on the global Internet
- In practice, they are and filters aren't being deployed (even when capability available)

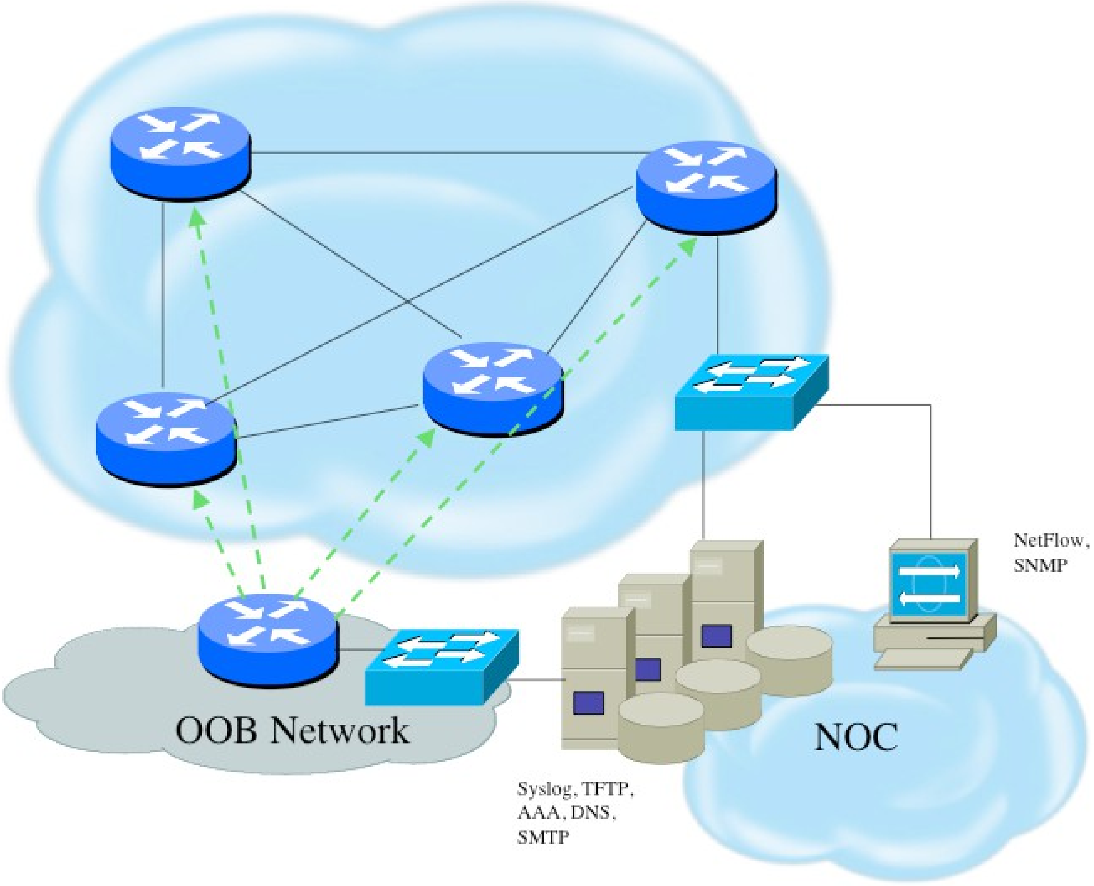


```
ipv6 access-list extended DSL-ipv6-Outbound
 permit ipv6 2001:DB8:AA65::/48  any
 deny   ipv6 any any log

interface atm 0/0
  ipv6 traffic-filter DSL-ipv6_Outbound out
```

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

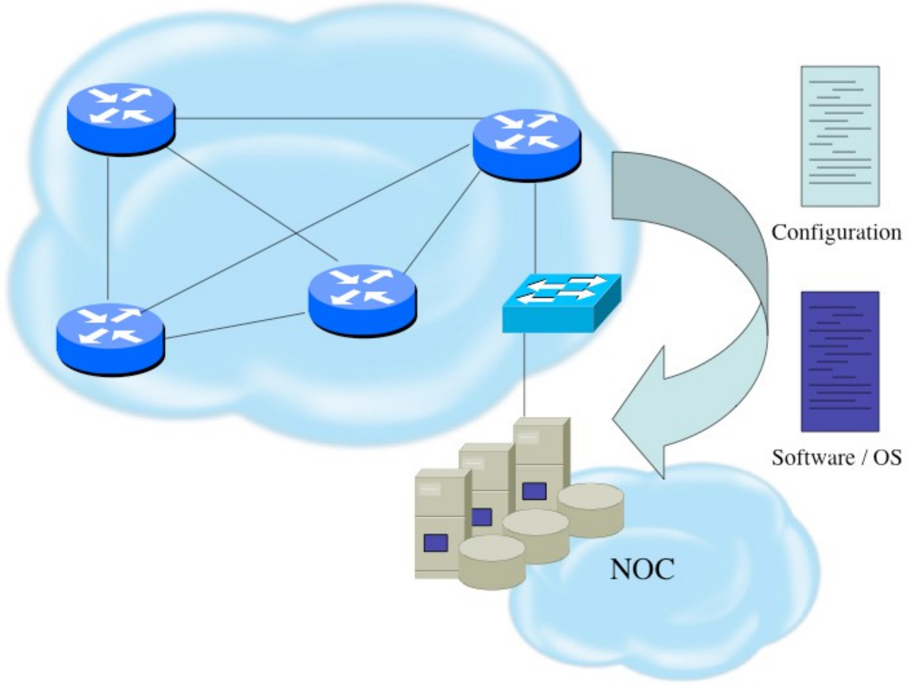
Device Management Common Practice

- 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 against modified configuration files

Software and Configuration Upgrade / Integrity



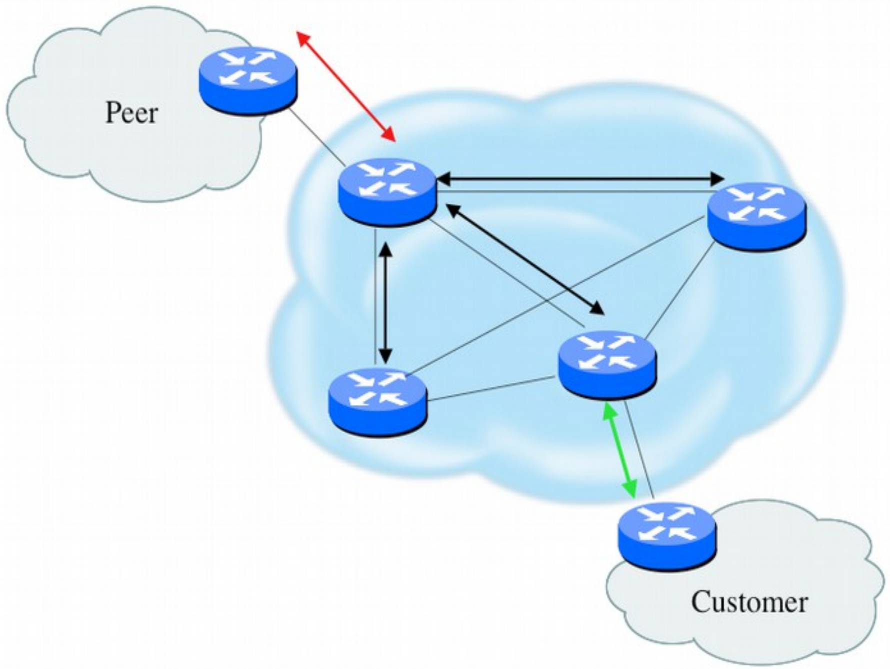
- Files stored on specific systems with limited access
- All access to these systems are authenticated and audited
- SCP is used where possible; FTP is NEVER used; TFTP still used
- Configuration files are polled and compared on an hourly basis (RANCID)
- Filters limit uploading / downloading of files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

Securing The Routing Infrastructure

Router Security Considerations

- Segment areas for route redistribution and ensure limited access to routers in critical backbone areas
- Design networks so outages don’t affect entire network but only portions of it
- Control router access….watch against internal attacks on these systems. Use different passwords for router enable and monitoring system root access.
- Scanning craze for all kinds of ports – this will be never ending battle

Routing Control Plane

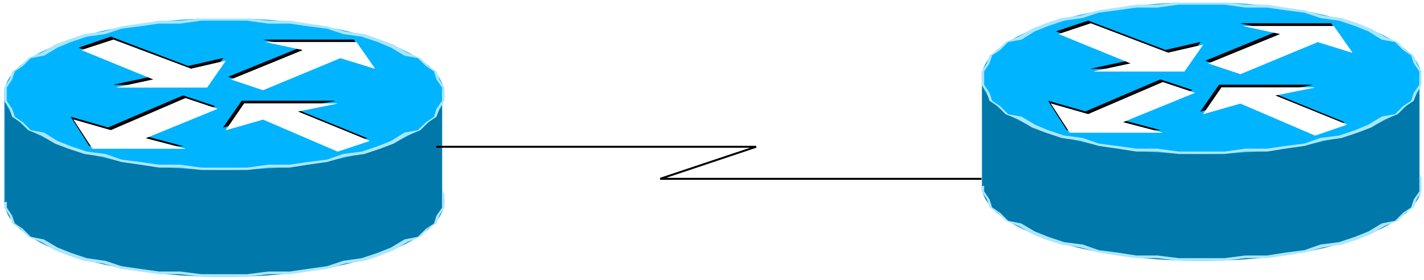


- MD-5 authentication
  - Some deploy at customer's request
- Route filters limit what routes are believed from a valid peer
- Packet filters limit which systems can appear as a valid peer
- Limiting propagation of invalid routing information
  - Prefix filters
  - AS-PATH filters (trend is leaning towards this)
  - Route dampening (latest consensus is that it causes more harm than good)
- Not yet possible to validate whether legitimate peer has authority to send routing update

Why Use Route Authentication

- Route Authentication equates to data origin authentication and data integrity
- In BGP, requires TCP resets to be authenticated so malicious person can't randomly send TCP resets
- In cases where routing information traverses shared networks, someone might be able to alter a packet or send a duplicate packet
- Routing protocols were not initially created with security in mind…..this needs to change….

Sample MD-5 Auth Configuration (OSPF)



```
interface Loopback0
ip address 70.70.70.70 255.255.255.255

interface Serial2
ip address 192.16.64.2 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 192.16.64.0 0.0.0.255 area 0
network 70.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
```

```
interface Loopback0
ip address 172.16.10.36 255.255.255.240

interface Serial1/0
ip address 192.16.64.1 255.255.255.0

ip ospf message-digest-key 1 md5 mk6
router ospf 10
network 172.16.0.0 0.0.255.255 area 0
network 192.16.64.0 0.0.0.255 area 0
area 0 authentication message-digest
```

Control Plane (Routing) Filters

- 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 filter lists

BGP Security Techniques

- BGP Community Filtering
- MD5 Keys on the eBGP and iBGP Peers
- Max Prefix Limits
- Prefer Customer Routes over Peer Routes (RFC 1998)
- GTSM (i.e. TTL Hack)

Audit and Validate Your Routing Infrastructures

- Are appropriate paths used?
  - check routing tables
  - verify configurations
- Is router compromised?
  - check access logs

Routing Security Conclusions

- Current routing protocols do not have adequate security controls
- Mitigate risks by using a combination of techniques to limit access and authenticate data
- Be vigilant in auditing and monitoring your network infrastructure
- Consider MD5 authentication
- Always filter routing updates….especially be careful of redistribution

But Wait…There's More…

- **RPKI** – Resource Public Key Infrastructure, the Certificate Infrastructure to Support the other Pieces
  - We need to be able to authoritatively prove who owns an IP prefix and what AS(s) may announce it
  - Prefix ownership follows the allocation hierarchy (IANA, RIRs, ISPs, etc)
- **Origin Validation** – Using the RPKI to detect and prevent mis-originations of someone else's prefixes (early 2012)
- **AS-Path Validation** AKA **BGPsec** – Prevent Attacks on BGP (future work)

BGP - Why Origin Validation?

- Prevent YouTube accident & Far Worse
- Prevents most accidental announcements
- Does not prevent malicious path attacks
- That requires ‘Path Validation’ and locking the data plane to the control plane, the third step, BGPsec

Infrastructure Security Summary

- Every device in your network could be exploited so make sure to harden them all (especially change default username/passwords)
  - printers, tablets, CPE's, etc
- Filtering help everyone – PLEASE deploy anti-spoofing filters
- Understand what you are sending in the clear from sending device to recipient and protect where needed
- Log and audit for trends since sometimes an abnormality can show the start of reconnaissance for a later attack