RSA Conference 2003

Attack on the Routing Protocols

Franjo Majstor
Cisco Systems, Inc.

Acknowledgment

- **Special thanks to:**

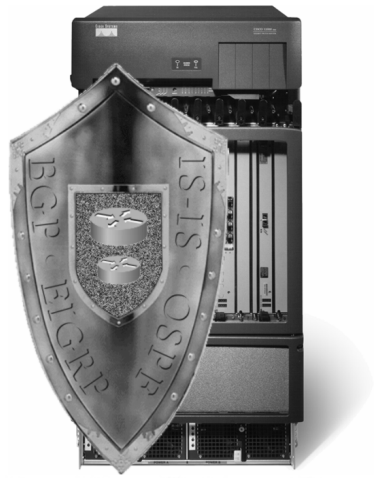
  Ido Dubrawsky from Cisco Systems for sharing the idea and the outcome of his research on this topic!

Introduction

- **Things you need to know:**
  - Basic concepts of routing, including path selection and filtering
  - Basic concepts of BGP, EIGRP, OSPF, and IS-IS is helpful
  - Basic concepts of internetwork connections and the Internet
  - Basic concepts of public key cryptography
- **And be aware of…**
  - "Internetwork Routing Protocol Attack Suite" (IRPAS) www.phenoelit.de/irpas/docu.html

Agenda

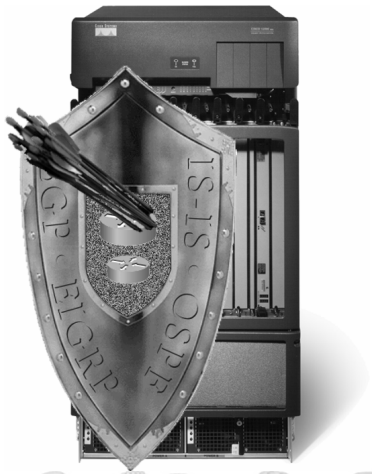
- **Attacks against Routing**
- **Protecting Routers**
- **Protecting Peering**
- **Filtering at the Network Edge**
- **Other**



Attacks against Routing

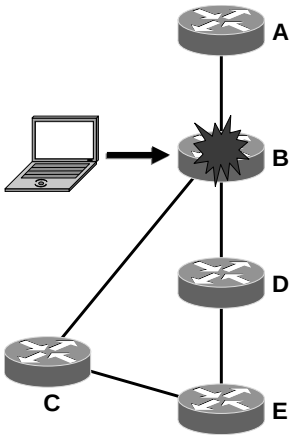
Agenda

- **Attacks against routing**
  - Disrupting Peering
  - Disrupting Routing
  - Attack Summary
- **Protecting Routers**
- **Protecting Peering**
- **Filtering at the Network Edge**
- **Other**



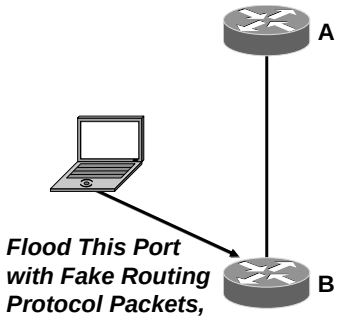
Disrupting Peering

- **Routing protocols describe peering relationships, methods of transferring data, and other semantics**
- **Attacks against a protocol can disrupt network usability through denial of service**
- **For instance, an attack against B can cause traffic from A and destined to E to be dropped rather than delivered**



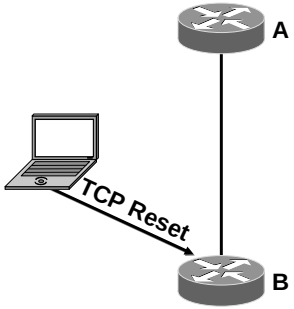
Disrupting Peering

- **Disrupting peering relationships is generally a matter of finding the address of a router in a critical location, and then attacking the router using normal DOS methods**
- **Disrupting peering through DOS attacks requires the ability to send packets to the router under attack**



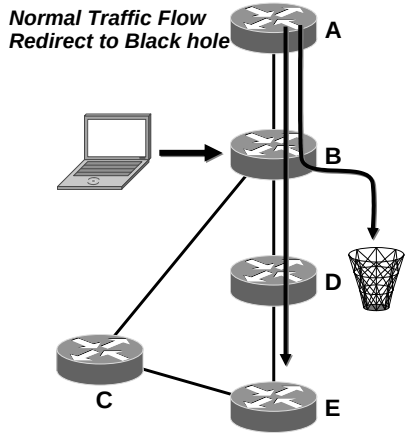
Disrupting Peering

- A more subtle attack is to force a peering session failure through malformed packets or state machine violations
- For instance, attacker can send a TCP reset to A and cause its peering session with B to fail
- Disrupting peering through malformed packets or state machine violations requires the ability to send packets to the router under attack



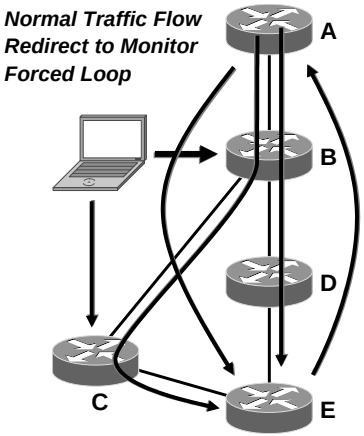
Disrupting Routing

- More subtle attacks involve attacking the information carried within the protocol, rather than the protocol itself
- For instance, the attacker may attempt to misdirect traffic into a black hole



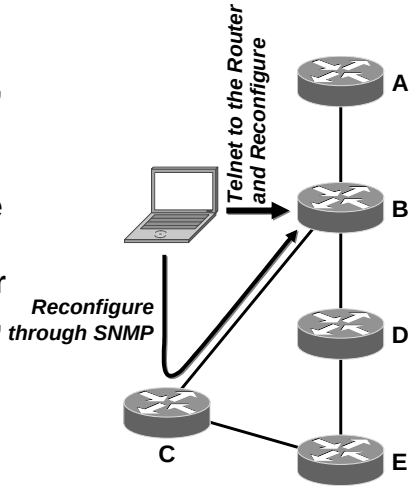
Disrupting Routing

- The attacker may misdirect traffic along a monitored path, so they can gain access to the information in the data stream
- The attacker may force a routing loop in the system, causing wide scale network outages
- Attacking the protocol in any of these ways requires some way to inject routing into the network



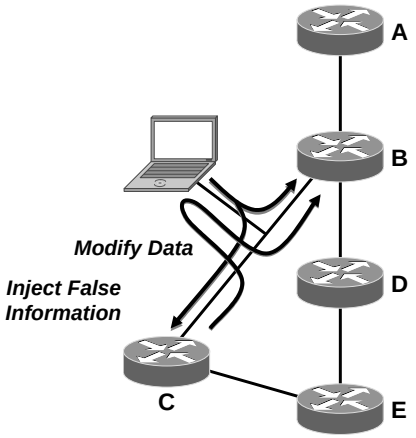
Disrupting Routing

- The attacker can compromise a router attached to the network, and use it to inject false routing information
- This requires being able to manipulate the configuration of a router attached to the network, possibly by gaining access to the console, setting configuration through SNMP, etc.



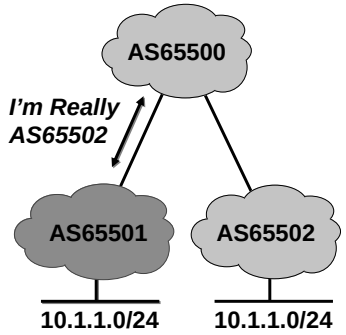
Disrupting Routing

- **The attacker can compromise the link between two routers, and inject false data, or modify data on the fly**
- **Injecting false routing information can include participating in the routing system**
- **For IGP's, this requires access to a link between two routers in the network, and the ability to modify or inject routing protocol packets**



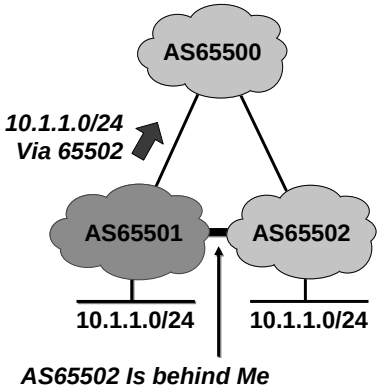
Disrupting Routing

- **In BGP terms, AS65501 would like to steal traffic destined to 10.1.1.0/24; What are its options?**
- **AS65501 can advertise that 10.1.1.0/24 is connected to it, as well as AS65502**
- **AS65501 can pretend to be AS65502**
  - Peer with 65500 using 65502 as its AS number



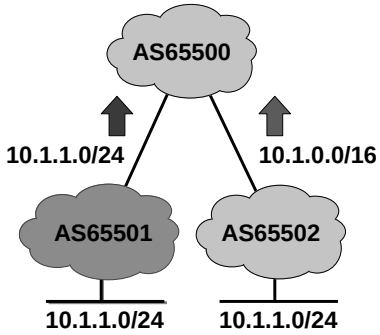
Disrupting Routing

- **AS65501 can advertise 10.1.1.0/24 with AS65502 in the AS path**
  - Peer with 65500 as 65501, but modify the AS path so 10.1.1.0/24 originates in 65502
- **AS65501 can pretend that AS65502 is actually reachable through it**
  - This isn't simple, since 65501 must convince 65500 that it's path to 10.1.1.0/24 is the best path



Disrupting Routing

- **If AS65502 isn't really advertising 10.1.1.0/24, but is rather advertising some aggregate of this prefix, AS65501 can easily convince AS65500 that it has the best path by advertising a longer prefix**



Attack Summary

- **An attacker must be able to:**
  - Source packets which are delivered to the router under attack
  - Configure a router through console access or some other means
  - Attach to the network and act as a part of the routing domain

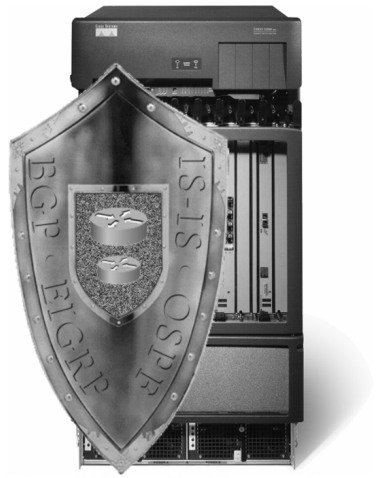
Protection

- **You need to protect:**
  - Routers from being compromised
  - Peering sessions between routers
  - The routing topology and reachability information from falsely injected information

Protecting Routers

Agenda

- **Attacks against Routing**
- **Protecting Routers**
- **Protecting Peering**
- **Filtering at the Network Edge**
- **Other**



Protecting Routers

- **One of the things an attacker always wants is access to one of the routers in your network**
- **You should deny them at every opportunity with security configured on the routers in your network**

Protecting Routers

- **Understand passwords, and privilege levels, and use them**
  - Cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/srprt5/srdpass.htm
- **Use SSH to connect to your routers, rather than telnet**
  - Cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/sshv1.htm#wp5038

```
ip ssh time-out 60
ip ssh authentication-retries 2
....
tacacs-server host 192.168.109.216
  port 9000
tacacs-server key cisco
radius-server host 192.168.109.216
  auth-port 1650 acct-port 1651
radius-server key 2difficult2guess
....
line con 0
 exec-timeout 0 0
 login authentication aaa7200kw
 transport input none
 access-group 10 in
....
enable secret 7 99ll89lkk98hhhjh
....
```

Protecting Routers

AutoSecure command in 12.3(1), 12.2(18)S

Cisco.com/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a008017d101.html

"One Touch" Device Lockdown

- **Simplify securing an IOS router and networks attached to an IOS router.**
  - –Built from security audit scripts and security whitepapers that Cisco and others provide. Large networks uses these to lock down their network.
- **Core Target is the CPE Routers on the edge of the Internet.**
  - –800/1700/2600/3600/3700 platforms, but applicable in large extent to all IOS platforms

AutoSecure : Global Services

- **Global Services turned off**
  - –Finger, PAD, Small Servers, Bootp, HTTP service, Identification Service, CDP, NTP, Source Routing
- **Global Services turned on**
  - – password-encryption service
  - – Tuning of scheduler interval/allocation
  - – tcp synwait-time
  - – tcp-keepalives-in and tcp-kepalives-out
  - – SPD configuration
  - – no ip unreachables for NULL0

AutoSecure : Services & Logging

- **Services Disabled Per Interface**

  ICMP
  Proxy-Arp
  Directed Broadcast -
  disables MOP service.
  disable icmp unreachables
  disable icmp mask reply messages.

- **Provide Logging for security**

  Enable sequence numbers & timestamp
  Provide a console log
  Set log buffered size
  Provide an interactive dialogue to configure the logging
  Log debug traffic

AutoSecure : Lockdown accessibility

- **Secure Access to the router**

  Check for a banner and provide facility to add text to Automatically Configure:

  - login, password
  - transport input & output
  - exec-timeout
  - local AAA
  - ssh timeout and ssh authentication-retries to minimum
  - enable only SSH,
  - SCP for access and file transfer to/from the router.
  - disables SNMP (if not being used.)

AutoSecure : Forwarding Plane

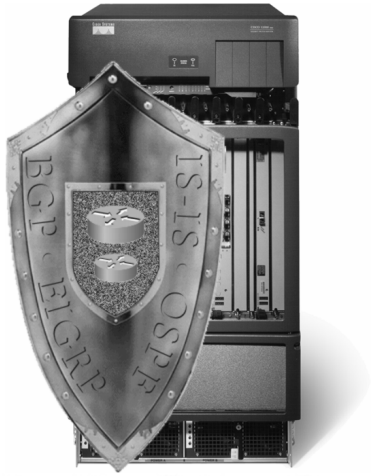
- **Securing the Forwarding Plane**

  - ✓ Enables Cisco Express Forwarding (CEF) or Distributed Cisco Express Forwarding (DCEF)
  - ✓ Anti-Spoofing
  - ✓ Block all IANA reserved ip address blocks.
  - ✓ Block private address blocks if customer desires
  - ✓ If not using a default route, install a default route to NULL 0.
  - ✓ If tcp intercept feature is available and user interested configure TCP intercept for connection-timeout.
  - ✓ If router is being used as firewall, start interactive configuration for CBAC on interfaces facing internet.
  - ✓ Enable netflow on software forwarding platforms.
  - ✓ Password Security.

Protecting Peering

Agenda

- **Attacks against Routing**
- **Protecting Routers**
- **Protecting Peering**
  - Peer Authentication
  - BGP TTL Security Hack
- **Filtering at the Edge**
- **Other**



Peer Authentication

- **MD5 peer authentication can protect against:**
  - Malformed packets tearing down a peering session
  - Unauthorized devices transmitting routing information
- **MD5 peer authentication cannot protect against:**
  - Reset routing protocol sessions due to denial of service attacks
  - Incorrect routing information being injected by a valid device which has been compromised
- **Neighbor Router Authentication: Overview and Guidelines contains a lot of good information about configuring and maintaining neighbor authentication**
  - Cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d2.html

Peer Authentication

- **OSPF supports MD5 digest signatures for authentication of data sent by peers**
  - Cisco.com/warp/public/104/25.shtml
- **IS-IS also supports MD5 digest signatures for authentication of data sent by peers**
  - Cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st21/ftmd5isi.htm

```
interface Serial 0/0
 ip address 192.168.64.2 255.255.255.0
 ip ospf message-digest-key key1
   md5 10a11b12c
 ip ospf authentication message-digest
 !
router ospf 10
 network 192.168.64.0 0.0.0.255 area 0
 area 0 authentication
```

```
key chain any%but%cisco
key 100
 key-string tasman-drive
!
interface Ethernet3
ip address 10.1.1.1 255.255.255.252
 ip router isis real_secure_network
 isis authentication mode md5 level-1
isis auth key-chain any%but%cisco level-1
!
router isis real_secure_network
 net 49.0000.0101.0101.0101.00
 is-type level-1
 authentication mode md5 level-1
 auth key-chain any%but%cisco level-1
```

Peer Authentication

- **EIGRP supports MD5 digest signatures for authentication data sent by peers**
  - Cisco.com/univercd/cc/td/doc/product/software/ios112/eigrpmd5.htm
- **BGP supports MD5 digest signatures for authentication data sent by peers**
  - Cisco.com/en/US/partner/about/ac123/ac114/ac173/ac170/about_cisco_packet_department09186a008010176a.html
- **MD5 on eBGP sessions requires coordinating with the other AS**

```
ip authentication key-chain eigrp 1 holly
key chain holly
 key 1
  key-string 0987654321
  accept-lifetime infinite
  send-lifetime ....
```

```
router bgp 109
neighbor 145.2.2.2 password v61ne0qkel33&
```

Peer Authentication

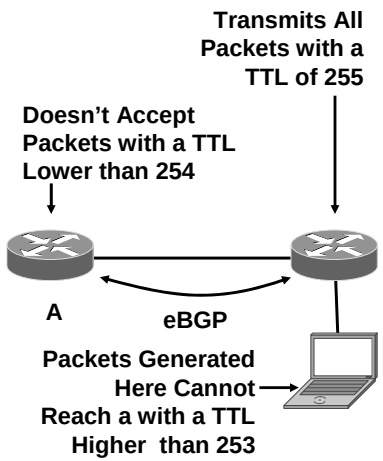
- RFC1321 describes MD5
  www.ietf.org/rfc/rfc1321.txt
- RFC3562 Key Management Considerations for the TCP MD5 Signature
  www.ietf.org/rfc/rfc3562.txt
- RFC2385 describes using MD5 with BGP
  www.ietf.org/rfc/rfc2385.txt

Peer Authentication

- MD5 does require intense processing on packets destined to the router
- It will limit the router's ability to process routing protocol packets destined to the router itself
- It doesn't impact the performance processing packets destined to the router which are not MD5 signed

BGP TTL Security Hack (BTSH)

- BTSH is a hack which protects the BGP peers from multihop attacks
- eBGP speakers are configured to transmit their packets with a TTL of 255, and to reject all packets with a TTL lower than 254 or 253
- A device which isn't connected between the BGP speakers cannot generate packets which will be accepted by either one of them

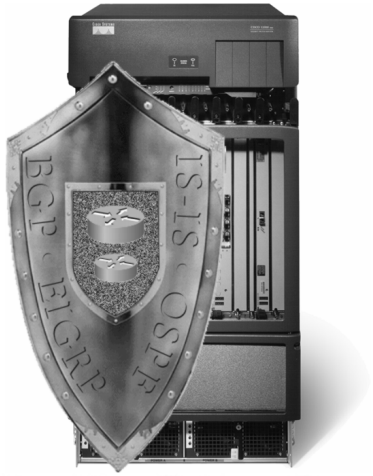


www.ietf.org/internet-drafts/draft-gill-btsh-02.txt

Filtering at the Edge

Agenda

- Attacks against Routing
- Protecting Routers
- Protecting Peering
- Filtering at the Network Edge
- Other



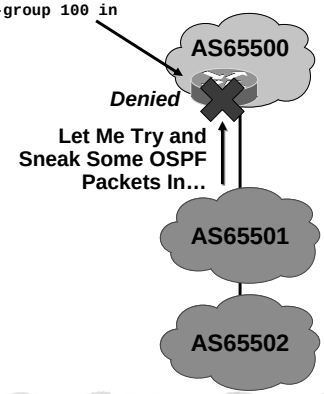
Filtering at the Edge

- **Never peer with an outside network using an IGP; always use BGP**
  - BGP is a policy-based protocol which expands your filtering options
  - BGP can take the abuses heaped on external connections
- **Goal is to prevent any invalid routing information from making it into your local routing tables using routing policy**
- **Use MD5 on any external BGP peering sessions, if possible**

Filtering at the Edge

- **Block all interior gateway protocol (OSPF and EIGRP) packets at the edge of your network**
- **This will protect against attackers trying to abuse routing protocols**

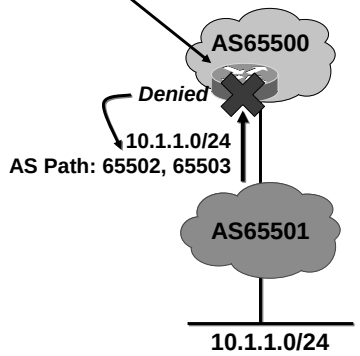
```
access-list 100 deny ospf any any
access-list 100 deny eigrp any any
access-list 100 permit ip any any
....
interface Serial 0
 ip access-group 100 in
```



Filtering at the Edge

- ***bgp enforce-first-as*** **prevents a BGP peer from advertising a route as if it is sourced from another autonomous system**
- **Use this with all peers!**
  - Cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008015ce53.html

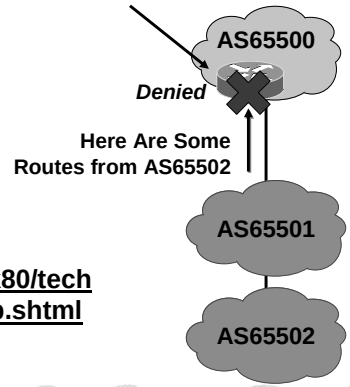
```
router bgp 65000
 bgp enforce-first-as
```



Filtering at the Edge

- **Use AS path filters to filter advertisements from partner and other peer routers**
- **Only use this if you don't want to accept full routes**

```
ip as-path access-list 10 permit ^65501$
!
router bgp 65000
 neighbor 10.1.1.1 filter-list 10 in
```

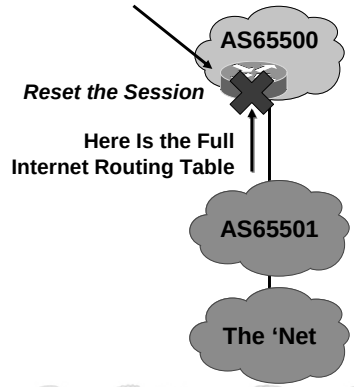


Cisco.com/en/US/partner/tech/tk365/tk80/technologies_tech_note09186a00801310cb.shtml

Filtering at the Edge

- **Limit the number of routes accepted at the edge**
- **This prevents dumping of large routing tables due to misconfiguration or attacks**
- **Consider each peer, and how many routes they should be advertising; for most partner peering sessions, the limit should be very small**
  - Cisco.com/en/US/partner/tech/tk826/tk365/technologies_configuration_example09186a008010a28a.shtml

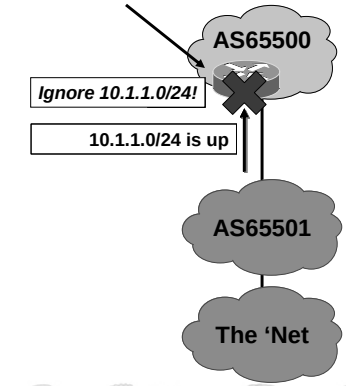
```
router bgp 65000
 neighbor 10.0.0.1 maximum-prefix 10 80
```



Filtering at the Edge

- **Dampen the routing information received from all BGP peers**
- **Damping protects you against constant route churn through network failures or used as an attack mechanism**
  - Cisco.com/en/US/partner/tech/tk826/tk365/technologies_tech_note09186a00800c95bb.shtml#flapdampen

```
router bgp 65000
 bgp dampening
```

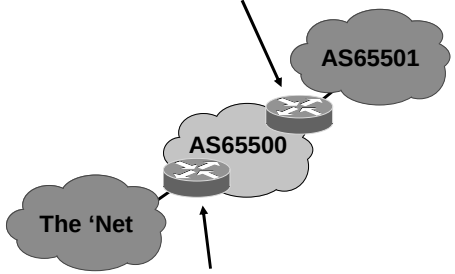


Filtering at the Edge

- **You should also filter out bogus routes at peering points with other networks**
- **Use filters for private peering specific to that peer**
- **Use filters for Internet peering to filter out common known bogus address spaces**
  - http://www.cisco.com/en/US/partner/tech/tk826/tk365/technologies_tech_note09186a00801310cb.shtml
  - http://www.cymru.com/Bogons/

```
ip prefix-list private permit 10.1.0.0/16 le 24

router bgp 65000
 neighbor 10.1.1.1 prefix-list private in
```

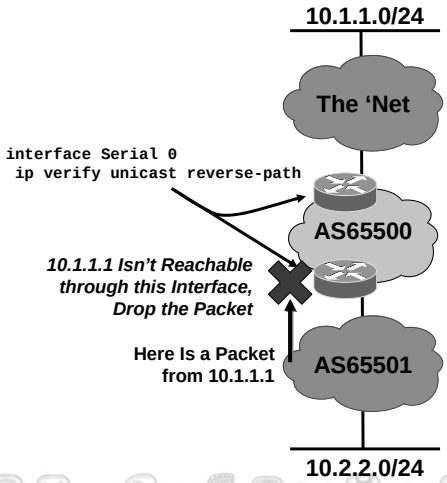



```
ip prefix-list public deny 0.0.0.0/0 ge 24
ip prefix-list public deny 10.1.0.0/16
ip prefix-list public deny 122.16.0.0/20
ip prefix-list public deny 192.168.0.0/16
ip prefix-list public permit 0.0.0.0/0

router bgp 65000
 neighbor 10.1.1.1 prefix-list public in
```

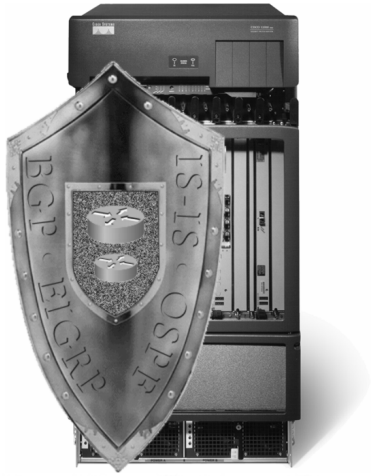
Filtering at the Edge

- **You should configure and use unicast reverse path forwarding checks at all edges**
  - http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d4.html
- **uRPF does require extra processing in the switching path of the router;**



Agenda

- **Attacks against Routing**
- **Protecting Routers**
- **Protecting Peering**
- **Filtering at the Network Edge**
- **Other**
  - soBGP
  - 802.1x



Secure Origin BGP (soBGP)

Design Constraints

- **So far, we've:**
  - Secured our routers
  - Secured our peering relationships
  - Filtered out unnecessary routing information from outside our network
  - Protected our edge routers from route flaps, excessive routes, etc.
- **None of this protects the information carried inside the routing protocol, however**

Design Constraints

- **We need something that will:**
  - Validate a given autonomous system is allowed to advertise a destination
  - Verify the peer we are learning the route from actually has a valid path to the destination
  - Verify the route against any policies the originating (Owning) autonomous system may have
- **Secure Origin BGP (soBGP), a proposed security system for the BGP protocol, meets these requirements**

soBGP

- **soBGP is currently in development**
- **ftp://ftp-eng.cisco.com/sobgp**
- **The mailing list is open, archives are available, draft participation is encouraged**

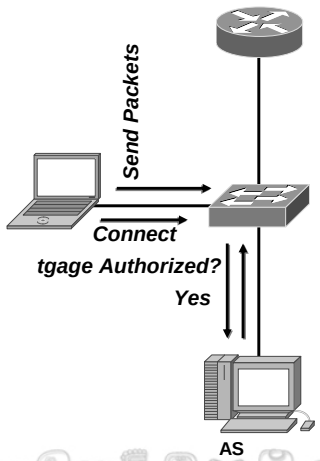
Why Call it soBGP?

- **Originally, soBGP was called soBGP because the primary focus we to validate the origin of prefixes within the routing system, and not worry about or emphasis valiting the path of an update so strongly. Over time, path validation has become a larger part of soBGP, and we are certain that other elements will be added…**

802.1x

Future Directions

- **802.1x layer 2 authentication can be used with TACACS+/RADIUS to authenticate users attaching to a network**
  - Cisco.com/en/US/partner/netsol/ns110/ns170/ns171/ns75/networking_solutions_package.html



Questions?

Thank you!

Attack on the Routing Protocols

Franjo Majstor,
Cisco Systems, Inc.