# Tutorial: Options for Blackhole and Discard Routing

**Joseph M. Soricelli**

**Wayne Gustavus**

**NANOG 32, Reston, Virginia**

# Caveats and Assumptions

- The views presented here are those of the authors and they do not necessarily represent the views of any other party
- This is a routing focused tutorial on ways to implement a security tool.
  - We won't be focusing on detection tools, types of attacks, analysis tools, etc.
- Basic understanding of OSPF, IS-IS and BGP
  - Route advertisements, BGP attributes, next-hop resolution
- Some configuration and output slides have been edited
- You will ask a question when you don't understand!

# Agenda

- Overview
- Discard options
- Mapping routes to blackholes
- Injecting and accepting routes
- Accounting and counting options

# Agenda

- → **Overview**
- ◆ Discard options
- ◆ Mapping routes to blackholes
- ◆ Injecting and accepting routes
- ◆ Accounting and counting options

# Why Blackhole Traffic?

- Mitigate denial of service (DoS) attacks
  - Prevention is another matter all together
- Protect vital network resources from outside attack
- Provide protection services for customers
  - Customer can initiate it’s own protection
- Log and track DoS attempts/attacks

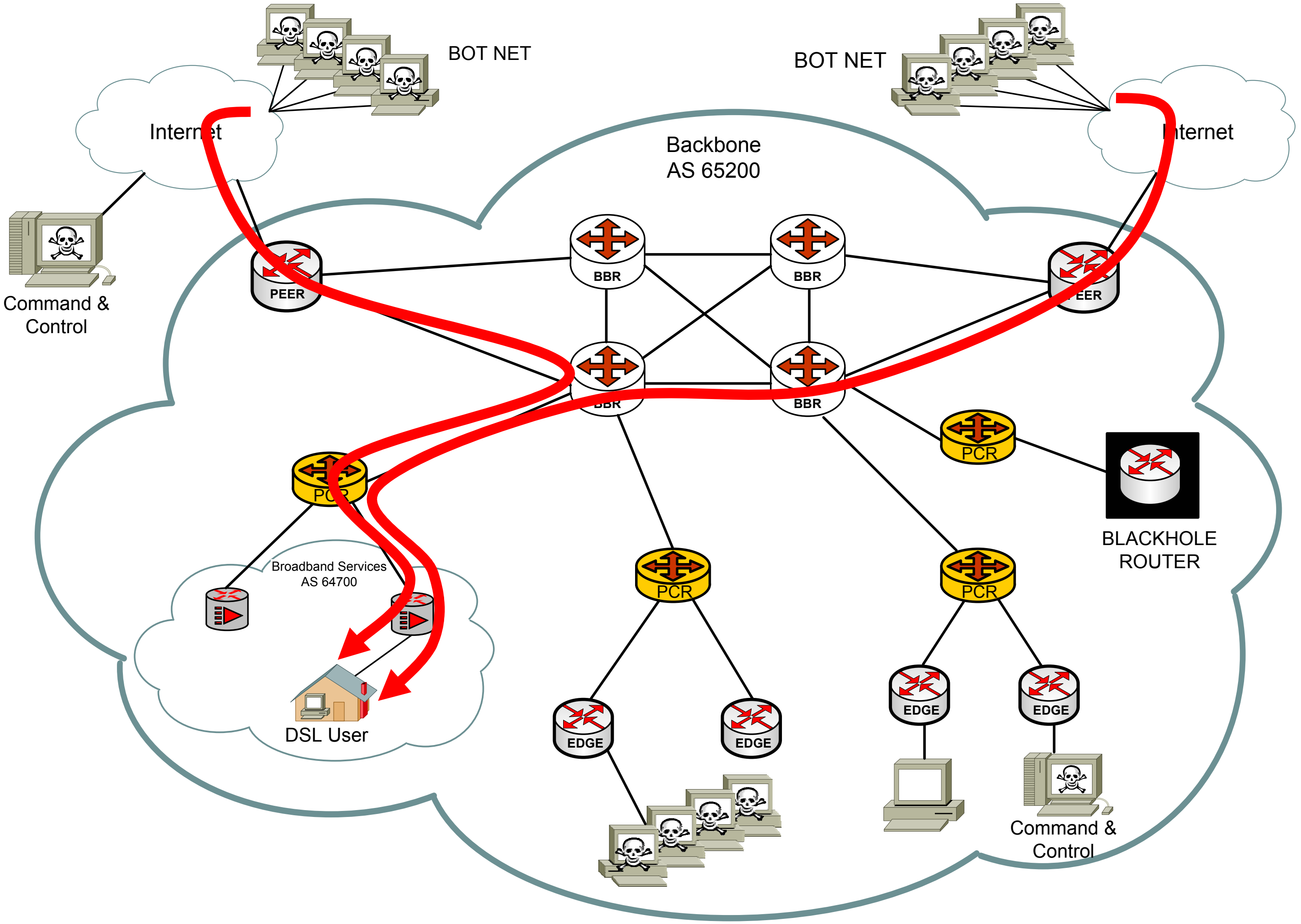
# Requirements for Blackhole Routing

- Effective overall plan
  - Routing policies and route maps
  - Discard interfaces and null static routes
  - Good internal routing knowledge
- Willingness to install a potentially complex (dangerous?) system
  - Policies / route maps on all routers in the network
  - Potential for misuse
- Operational Guidelines
  - Strict access control and command logging
  - Audits to clean up stale blackhole routing
  - Integrate with existing NMS

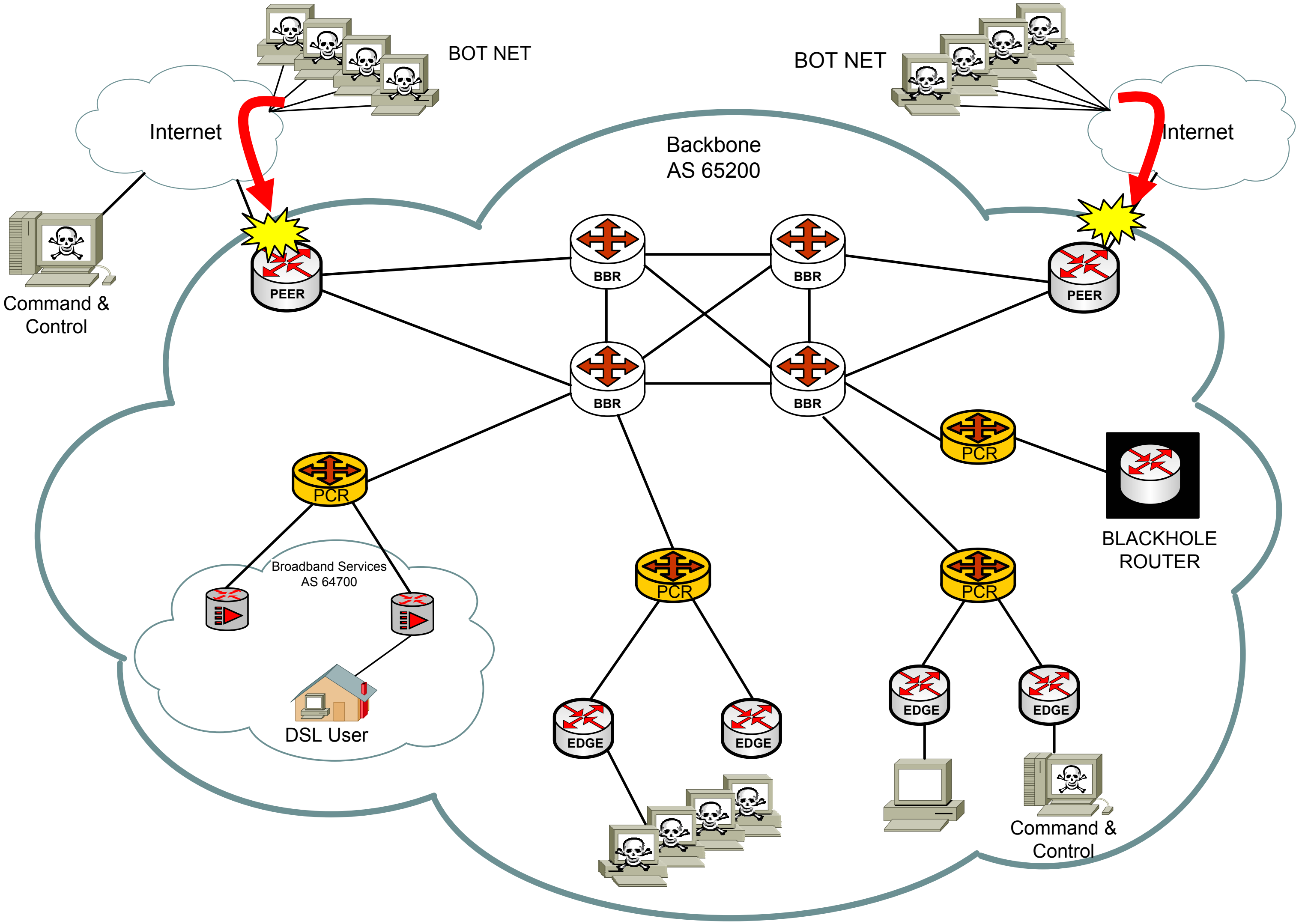
# Who Should Be Blackholed?

- Attacks to customers
  - From peers and/or other customers
- Attacks from customers
  - To peers and/or other customers
- Attack Controllers
  - Hosts providing attack instructions
- Unallocated address spaces?
  - BOGONS

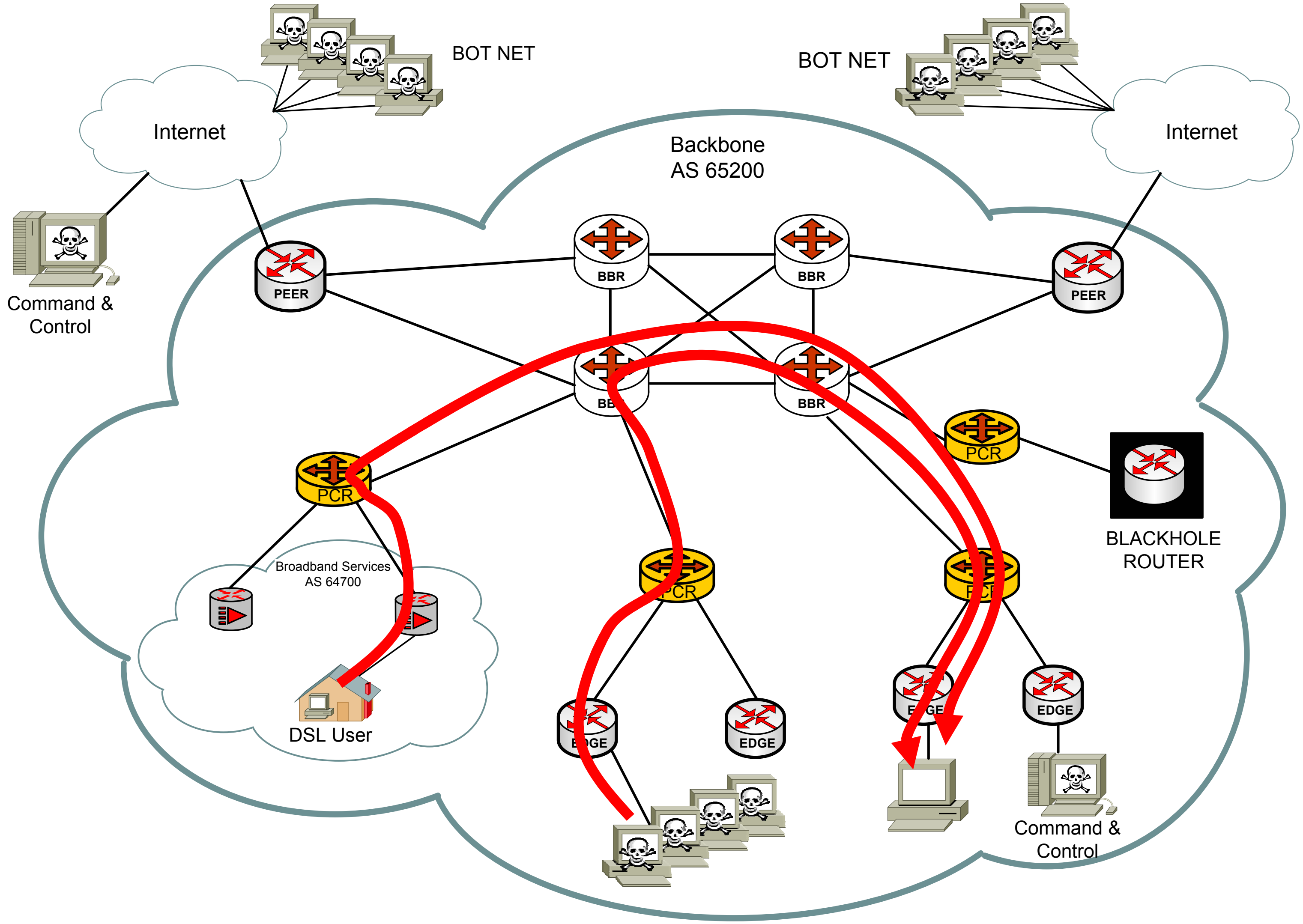
# Attacks Towards Customer



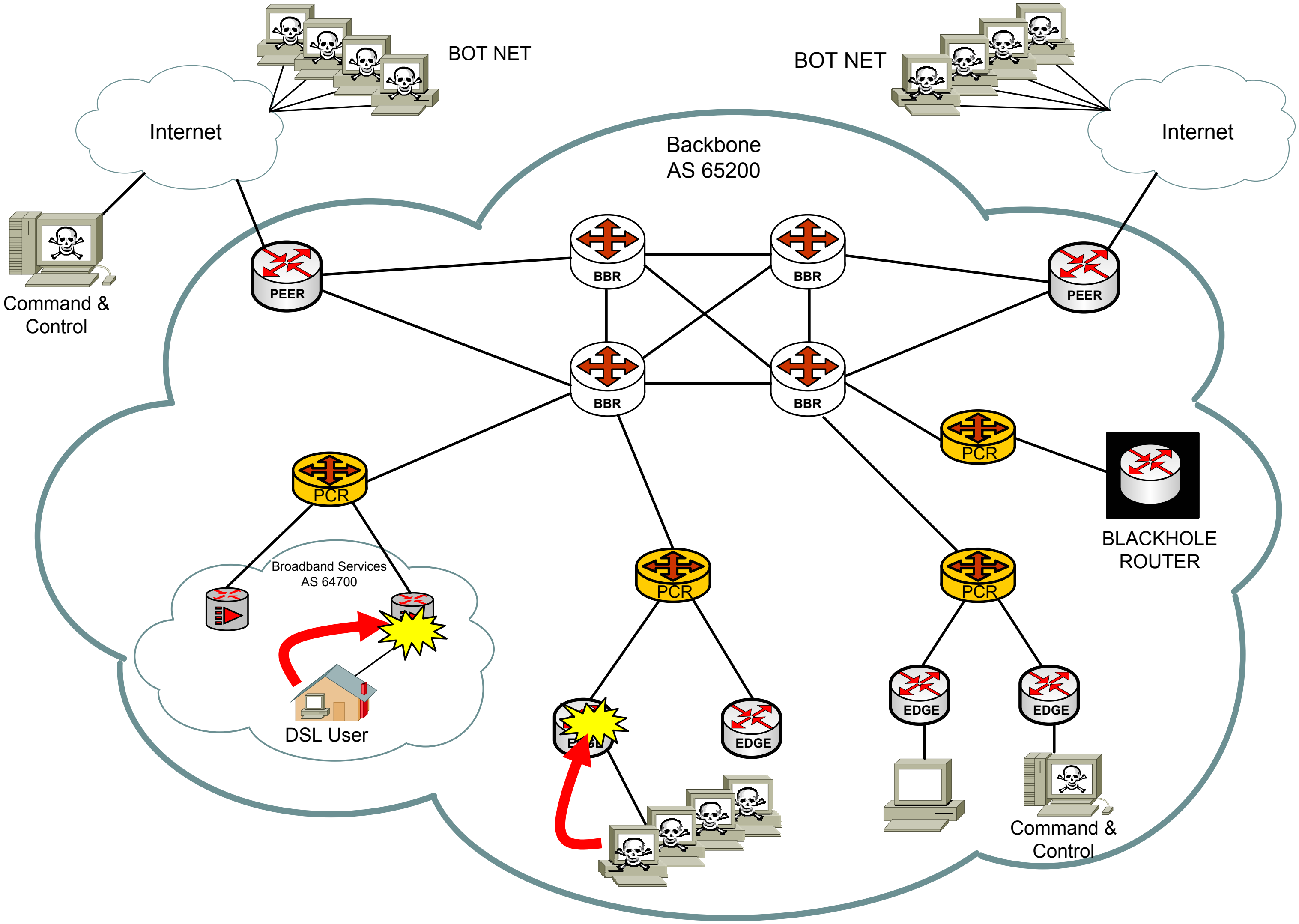
# Attacks Towards Customer—Blackholed!



# Attacks From Customers

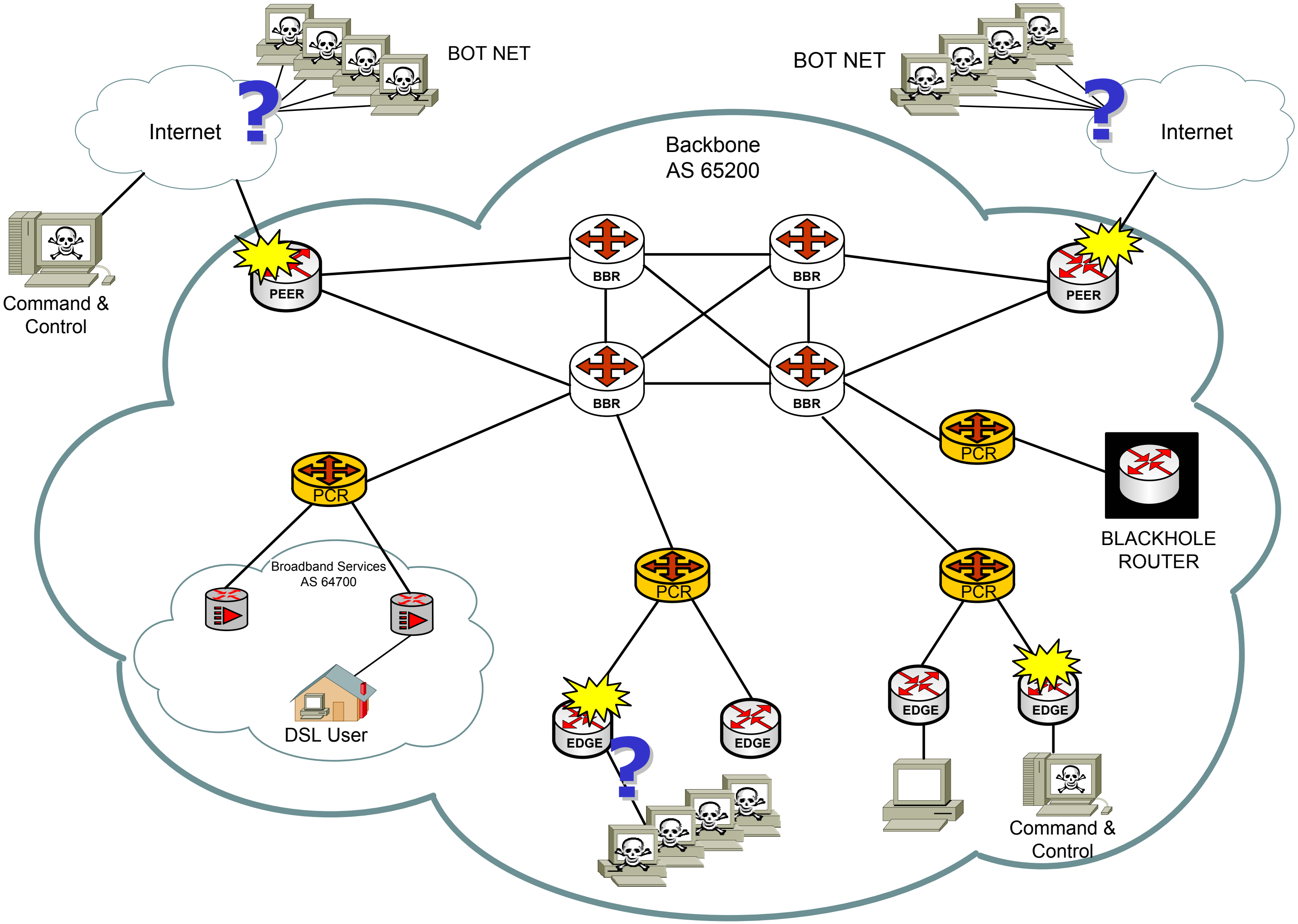


# Attacks From Customers—Blackholed!



17 October 2004

# Attack Controllers—Blackholed!



# Agenda

- Overview
- ➔ **Discard options**
- Mapping routes to blackholes
- Injecting and accepting routes
- Accounting and counting options

# Discard/Reject Static Route

- On Juniper routers, create a static route for each next-hop used for blackholed routes
  - Select either discard or reject as the next-hop action
  - Be cautious of ICMP rate-limiting with reject action!

```
user@host> show configuration routing-options
static {
route 192.0.2.101/32 discard;
    route 192.0.2.103/32 reject;
    route 192.0.2.105/32 discard;
}

user@host> show route protocol static terse

inet.0: 24 destinations, 24 routes (24 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination          P Prf   Metric 1   Metric 2  Next hop        AS path
* 192.0.2.101/32       S   5                        Discard
* 192.0.2.103/32       S   5                        Reject
* 192.0.2.105/32       S   5                        Discard
```

# Null 0 Static Route

- **On Cisco routers, create a separate static route to Null 0 for each next-hop you are assigning to the blackhole routes**

```
ip route 192.0.2.101 255.255.255.255 Null0
ip route 192.0.2.103 255.255.255.255 Null0
ip route 192.0.2.105 255.255.255.255 Null0

ISP-BLKHOLE-RTR1#sh ip route 192.0.2.0
Routing entry for 192.0.2.0/32, 3 known subnets
  Attached (3 connections)

S       192.0.2.103 is directly connected, Null0
S       192.0.2.101 is directly connected, Null0
S       192.0.2.105 is directly connected, Null0
ISP-BLKHOLE-RTR1#
```

# Discard Interface

- Alternatively on a Juniper router, create a discard interface which contains the next-hop you are assigning to the blackhole routes
  - Multiple IP addresses on a single logical unit
  - Use of the `destination` command works best

- This allows you to configure and assign filters to the interface for counting, logging, and sampling the traffic
  - Only a discard next-hop action is used

# Discard Interface

```
user@host> show configuration interfaces dsc
unit 0 {
    family inet {
        address 192.0.2.102/32 {
            destination 192.0.2.101;
        }
        address 192.0.2.104/32 {
            destination 192.0.2.103;
        }
        address 192.0.2.106/32 {
            destination 192.0.2.105;
        }
    }
}
```

```
user@host> show interfaces terse dsc
Interface               Admin Link Proto Local                 Remote
dsc                     up    up
dsc.0                   up    up   inet  192.0.2.102         --> 192.0.2.101
                                         192.0.2.104         --> 192.0.2.103
                                         192.0.2.106         --> 192.0.2.105
```

# Agenda

- ◆ Overview
- ◆ Discard options
- → **Mapping routes to blackholes**
- ◆ Injecting and accepting routes
- ◆ Accounting and counting options

# Mapping Routes to Blackhole Services

- To actually blackhole packets requires either a routing policy or a route map attached to the BGP sessions
- Blackhole eligible packets must be located
  - Use a route-filter or access list to locate individual routes (administratively hard)
  - Use a BGP community value (quite scalable)

# Locating Specific Routes w/ Route-Filter

```
protocols {
    bgp {
        import blackhole-by-route;
    }
}
policy-options {
    policy-statement blackhole-by-route {
        term specific-routes {
            from {
                route-filter 10.10.10.1/32 exact;
                route-filter 10.20.20.2/32 exact;
                route-filter 10.30.30.3/32 exact;
                route-filter 10.40.40.4/32 exact;
            }
            then {
                next-hop 192.0.2.101
            }
        }
    }
}
```

# Locating Specific Routes w/ Access List

```
access-list 88 remark Bogon Filter List: v2.4 28 Apr 2004
access-list 88 permit 0.0.0.0 1.255.255.255
access-list 88 permit 2.0.0.0 0.255.255.255
access-list 88 permit 5.0.0.0 0.255.255.255
access-list 88 permit 7.0.0.0 0.255.255.255
access-list 88 permit 10.0.0.0 0.255.255.255
access-list 88 permit 23.0.0.0 0.255.255.255
access-list 88 permit 27.0.0.0 0.255.255.255
access-list 88 permit 31.0.0.0 0.255.255.255
access-list 88 permit 36.0.0.0 1.255.255.255
access-list 88 permit 39.0.0.0 0.255.255.255
.
.
etc (good source is BOGON route object (fltr-bogons) in RADB)

route-map BLKHOLE-ROUTES-IN permit 10
 match ip address 88
 set ip next-hop 192.0.2.101
!
neighbor 172.16.1.1 route-map BLKHOLE-ROUTES-IN in
```

# Use Communities to Locate Routes

```
protocols {
    bgp {
        import blackhole-policy;
    }
}
policy-options {
    policy-statement blackhole-policy {
        term blackhole-communities {
            from {
                community blackhole-all-routers;
}
            then {
                next-hop 192.0.2.101
            }
        }
    }
    community blackhole-all-routers members 65200:55..$
}
```

# Use Communities to Locate Routes

- **Different Community Regular Expression**
  - **JUNOS/IOS Implementations Differ**
  - **IOS: Regex applies to entire set of values**
  - **JUNOS: Regex applies to individual community**

```
ip community-list expanded BLKHOLE-ALL-ROUTERS permit 65200:55.._

route-map BLKHOLE-ROUTES-IN permit 10
 match community BLKHOLE-ALL-ROUTERS
 set ip next-hop 192.0.2.101
!
neighbor 172.16.1.1 route-map BLKHOLE-ROUTES-IN in
```

# Blackhole Communities

- A clear list of possible communities is needed
  - Easier troubleshooting and operation
  - Better security
- Some hierarchy and stratification is good
  - Routes accepted from customers (5500-5509)
  - Injected customer routes (5520-5529)
  - Injected BOGON routes (5530-5539)
  - Injected provider routes (5540-5549)

# Blackhole Communities

- CUST-ANNOUNCE-BLKHOLE-ALL
  - 65200:5501
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
- CUST-ANNOUNCE-BLKHOLE-PEER
  - 65200:5503
  - Next-hop set to 192.0.2.103
  - Packets are dropped on Peer routers only
  - Allows customer to stop attacks from off-net while continuing flows from other on-net connections

# Blackhole Communities

- ISP-BLKHOLE-CUST-ALL
  - 65200:5521
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
- ISP-BLKHOLE-CUST-PEER
  - 65200:5523
  - Next-hop set to 192.0.2.103
  - Packets are dropped on Peer routers only
- ISP-BLKHOLE-CUST-CORE
  - 65200:5525
  - Next-hop set to 192.0.2.105
  - Packets are dropped on all but Edge routers

# Blackhole Communities

- ISP-BLKHOLE-BOGON-MARTIAN
  - 65200:5530
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes include things like 127/8, 128.0/16, and 192.0.0/24
- ISP-BLKHOLE-BOGON-RFC-1918
  - 65200:5531
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes are 10/8, 172.16/12, and 192.168/16

# Blackhole Communities

- ISP-BLKHOLE-BOGON-IANA-RSVD
  - 65200:5532
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes match the list of current reserved addresses
- ISP-BLKHOLE-BOGON-PUBLIC-EXCHANGE
  - 65200:5533
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes include subnet addresses from public peering points the ISP is not attached to

# Blackhole Communities

- ISP-BLKHOLE-INFRA-PEERING-LINKS
  - 65200:5540
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes include the peering connections of the ISP
- ISP-BLKHOLE-INFRA-LAN
  - 65200:5541
  - Next-hop set to 192.0.2.101
  - Packets are dropped on all possible routers
  - Routes include subnet addresses for protected internal services

# Using EBGP Multihop

- By default, next-hop must equal the EBGP peer address
- Altering the next-hop for blackhole services requires multihop on the EBGP sessions

# Multihop Configurations – Edge/Peer

```
protocols {
    bgp {
        group EBGP-Peers {
            neighbor 172.16.1.1;
            type external;
            peer-as 65432;
            multihop;
            local-address 172.16.254.254;
            import blackhole-policy-edge;
        }
    }
}

router bgp 65200
 neighbor 172.16.1.1 remote-as 65432
 neighbor 172.16.1.1 description “ISP CORE-RTR1"
 neighbor 172.16.1.1 ebgp-multihop 2
 neighbor 172.16.1.1 send-community
 neighbor 172.16.1.1 route-map BLKHOLE-POLICY-EDGE in
```

# Agenda

- Overview
- Discard options
- Mapping routes to blackholes
- → **Injecting and accepting routes**
- Accounting and counting options

# Injecting Routes: Blackhole Router

- Bogon Routes
  - Manual injection of bogons (martians, rfc1918, IANA)
  - Managing external feed for automatic updates

- Host Routes
  - Injecting /32 routes for AUP violations
  - Tracking mechanisms (integrate w/ NMS)
  - Audit procedures (keeping dynamic pools fresh!)

# Blackhole Router Configs: Communities

```
policy-options {
    community CUST-ANNOUNCE-BLKHOLE-ALL members 65200:5501;
    community CUST-ANNOUNCE-BLKHOLE-PEER members 65200:5503;
    community ISP-BLKHOLE-CUST-ALL members 65200:5521;
    community ISP-BLKHOLE-CUST-PEER members 65200:5523;
    community ISP-BLKHOLE-CUST-CORE members 65200:5525;
    community ISP-BLKHOLE-BOGON-MARTIAN members 65200:5530;
    community ISP-BLKHOLE-BOGON-RFC-1918 members 65200:5531;
    community ISP-BLKHOLE-BOGON-IANA-RSVD members 65200:5532;
    community ISP-BLKHOLE-BOGON-PUBLIC-EXCHANGE members 65200:5533;
    community ISP-BLKHOLE-INFRA-PEERING-LINKS members 65200:5540;
    community ISP-BLKHOLE-INFRA-LAN members 65200:5541;
}

ip community-list expanded CUST-ANNOUNCE-BLKHOLE-ALL permit 65200:5501
ip community-list expanded CUST-ANNOUNCE-BLKHOLE-PEER permit 65200:5503
ip community-list expanded ISP-BLKHOLE-CUST-ALL permit 65200:5521
ip community-list expanded ISP-BLKHOLE-CUST-PEER permit 65200:5523
ip community-list expanded ISP-BLKHOLE-CUST-CORE permit 65200:5525
ip community-list expanded ISP-BLKHOLE-BOGON-MARTIAN permit 65200:5530
ip community-list expanded ISP-BLKHOLE-BOGON-RFC-1918 permit 65200:5531
ip community-list expanded ISP-BLKHOLE-BOGON-IANA-RSVD permit 65200:5532
ip community-list expanded ISP-BLKHOLE-BOGON-PUBLIC-EXCHANGE permit 65200:5533
ip community-list expanded ISP-BLKHOLE-INFRA-PEERING-LINKS permit 65200:5540
ip community-list expanded ISP-BLKHOLE-INFRA-LAN permit 65200:5541
```

# Blackhole Router Configs: Prefix Lists

```
policy-options {
    prefix-list BOGON-MARTIAN {
        0.0.0.0/8;
        127.0.0.0/8;
        128.0.0.0/16;
        169.254.0.0/16;
        191.255.0.0/16;
        192.0.0.0/24;
        192.0.2.0/24;
        198.18.0.0/15;
        223.255.255.0/24;
        224.0.0.0/3;
    }
    prefix-list BOGON-RFC-1918 {
        10.0.0.0/8;
        172.16.0.0/12;
        192.168.0.0/16;
    }
}
```

# Blackhole Router Configs: Prefix Lists

```
ip prefix-list BOGON-MARTIAN seq 10 permit 0.0.0.0/8
ip prefix-list BOGON-MARTIAN seq 20 permit 127.0.0.0/8
ip prefix-list BOGON-MARTIAN seq 30 permit 128.0.0.0/16
ip prefix-list BOGON-MARTIAN seq 40 permit 169.254.0.0/16
ip prefix-list BOGON-MARTIAN seq 50 permit 191.255.0.0/16
ip prefix-list BOGON-MARTIAN seq 60 permit 192.0.0.0/24
ip prefix-list BOGON-MARTIAN seq 70 permit 192.0.2.0/24
ip prefix-list BOGON-MARTIAN seq 80 permit 198.18.0.0/15
ip prefix-list BOGON-MARTIAN seq 90 permit 223.255.255.0/24
ip prefix-list BOGON-MARTIAN seq 100 permit 224.0.0.0/3
ip prefix-list BOGON-MARTIAN seq 1000 deny 0.0.0.0/0

ip prefix-list BOGON-RFC-1918 seq 10 permit 10.0.0.0/8
ip prefix-list BOGON-RFC-1918 seq 20 permit 172.16.0.0/12
ip prefix-list BOGON-RFC-1918 seq 30 permit 192.168.0.0/16
ip prefix-list BOGON-RFC-1918 seq 100 deny 0.0.0.0/0
```

# Blackhole Router Configs: Policies

```
policy-options {
    policy-statement ADV-BOGON-ROUTES {
        term MARTIANS {
            from prefix-list BOGON-MARTIAN;
            then {
                community add ISP-BLKHOLE-BOGON-MARTIAN;
                accept;
            }
        }
        term RFC-1918 {
            from prefix-list BOGON-RFC-1918;
            then {
                community add ISP-BLKHOLE-BOGON-RFC-1918;
                accept
            }
        }
    }
}

route-map ADV-BOGON-ROUTES permit 10
 match ip address prefix-list BOGON-MARTIAN
 set community 65200:5530
!
route-map ADV-BOGON-ROUTES permit 20
 match ip address prefix-list BOGON-RFC-1918
 set community 65200:5531
```

# Accepting Customer Routes: Edge Rtr

- Policies and route maps should be in place to only accept routes from the customer's allocation
  - Keeps customer from blackholing other's routes

- Blackhole policies should be added to accept routes with known communities and alter the next-hop
  - Could be set to allow a range of subnet mask lengths
  - Most effective when all possible mask lengths are accepted

# Accepting Customer Routes: Edge Rtr

```
policy-options {
    policy-statement blackhole-policy-edge {
        term CUST-ROUTES-ALL-ROUTERS {
            from {
                protocol bgp;
                community CUST-ANNOUNCE-BLKHOLE-ALL;
            }
            then {
                next-hop 192.0.2.101;
                accept;
            }
        term CUST-ROUTES-PEER-ROUTERS {
            from {
                protocol bgp;
                community CUST-ANNOUNCE-BLKHOLE-PEER;
            }
            then {
                next-hop 192.0.2.103;
                accept;
            }
        }
    }
}
```

# Accepting Customer Routes: Edge Rtr

```
ip prefix-list CUSTOMER-ROUTES seq 10 permit 172.16.1.0/24 le 32
ip prefix-list CUSTOMER-ROUTES seq 1000 deny 0.0.0.0/0

ip community-list expanded CUST-ANNOUNCE-BLKHOLE-ALL permit 65200:5501
ip community-list expanded CUST-ANNOUNCE-BLKHOLE-PEER permit 65200:5503
!
route-map BLKHOLE-POLICY-EDGE permit 10
 match community CUST-ANNOUNCE-BLKHOLE-ALL
 set ip next-hop 192.0.2.101
!
route-map BLKHOLE-POLICY-EDGE permit 20
 match community CUST-ANNOUNCE-BLKHOLE-PEER
 set ip next-hop 192.0.2.103
!
route-map BLKHOLE-POLICY-EDGE permit 30
 match ip address prefix-list CUSTOMER-ROUTES
```

# The End Result

```
user@host> show route 10.104.252.227/32 detail
10.104.252.227/32 (2 entries, 1 announced)
        *BGP    Preference: 170/-101
                Source: 172.16.1.1
                Next hop: 192.0.2.1 via dsc.0, selected
                Protocol next hop: 192.0.2.1 Indirect next hop: f0b8930 1134
                State: <Active Int Ext>
                Local AS: 65200 Peer AS: 65200
                Age: 4:25:24    Metric: 0       Metric2: 0
                Task: BGP_65200.130.81.254.21+179
                AS path: 65334 I (Originator) Cluster list:  172.16.1.1
                AS path:  Originator ID: 172.16.1.1
                Communities: 65200:999 65200:5521
                Localpref: 100
                Router ID: 172.16.1.1
```

# Also: Dropping Based on Source Address

- **Use blackhole routes to drop by source address**
  - **Relies on unicast reverse path check (RPF)**
  - **RPF treats blackhole routes as invalid**
  - **Can verify with syslog data or debug (debug ip cef drop verify)**

```
interface ATM1/0/0.5500 point-to-point
 ip verify unicast reverse-path
!
rtr#debug ip cef drop verify
!
Sep 23 11:38:47.353 UTC: CEF-Drop: Packet from 127.0.0.1 via
ATM1/0/0.5500 -- ip verify check
Sep 23 11:38:50.333 UTC: CEF-Drop: Packet from 127.0.0.1 via
ATM1/0/0.5500 -- ip verify check
Sep 23 11:39:02.430 UTC: CEF-Drop: Packet from 127.0.0.1 via
ATM1/0/0.5500 -- ip verify check
```

# Agenda

- Overview
- Discard options
- Mapping routes to blackholes
- Injecting and accepting routes

→ **Accounting and counting options**

# Seeing What Is Blackholed

- Other methods besides examining the route table to determine what is being blackholed
  - Especially useful for counting packets and examining packet headers
- Outbound filter applied to the discard interface
  - Counting
  - Logging
  - Syslog
- Sampling can also be performed
  - Within the filter or on the interface

# Null 0 Static Route and Netflow

- **While a Cisco router can only blackhole traffic to a single interface (Null0), there is still value in using multiple IP destinations**
  - **Netflow data provides visibility into traffic types for each destination**

```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         192.168.51.1    Null          192.0.2.105     01 0000 0800     5
```

# Simple Discard Interface Filter

```
user@host> show configuration interfaces dsc
unit 0 {
    family inet {
        filter {
            output blackhole-filter;
        }
        address 192.0.2.102/32 {
            destination 192.0.2.101;
        }
        address 192.0.2.104/32 {
            destination 192.0.2.103;
        }
        address 192.0.2.106/32 {
            destination 192.0.2.105;
        }
    }
}
user@host> show configuration firewall filter blackhole-filter
term blackhole-accounting {
    then {
        count blackholed-packets;
        sample;
        discard;
    }
}
```

# Simple Discard Interface Filter Issues

- The "problem" with using a single blackhole filter is visibility
  - All blackholed packets increment the same counter
- To see which categories of packets are being blackholed, use destination class usage (DCU)
  - Associates a user-defined class with each blackhole community
  - The DCU classes are then referenced in a firewall filter

# DCU and Blackhole Filters

```
routing-options {
    forwarding-table {
        export map-blackhole-communities-to-dcu-classes;
    }
}
policy-options {
    policy-statement map-blackhole-communities-to-dcu-classes {
        term CUST-BLKHOLE-ALL {
            from community CUST-ANNOUNCE-BLKHOLE-ALL;
            then destination-class CUST-BLKHOLE-ALL-DCU;
        }
        term CUST-BLKHOLE-PEER {
            from community CUST-ANNOUNCE-BLKHOLE-PEER;
            then destination-class CUST-BLKHOLE-PEER-DCU;
        }
    }
}
```

# DCU and Blackhole Filters

```
firewall {
    filter blackhole-filter {
        term CUST-BLKHOLE-ALL
            from {
                destination-class CUST-BLKHOLE-ALL-DCU;
            }
            then {
                count CUST-BLKHOLE-ALL-COUNT;
                sample;
                discard;
            }
        }
        term CUST-BLKHOLE-PEER
            from {
                destination-class CUST-BLKHOLE-PEER-DCU;
            }
            then {
                count CUST-BLKHOLE-PEER-COUNT;
                sample;
                discard;
            }
        }
    }
}
```

# DCU and Blackhole Filters

```
user@host> show firewall filter blackhole-filter
Filter: blackhole-filter
Counters:
Name                                                Bytes              Packets
CUST-BLKHOLE-ALL-COUNT                              11444                  357
CUST-BLKHOLE-PEER-COUNT                             91468                 1871
```

# Questions and Comments

- Feedback on this presentation is highly encouraged
  - jms@juniper.net
  - wgustavus@gnilink.net

- Questions?

Thank you!