Raising the Bar for the Attacker

Blocking Pivoting with Wildcard Masks, ACLs, and PVLANs

Greg Scheidel (@greg_scheidel)

What Does Nirvana Look Like?

Defensible Network [1]

- Limits an Intruder's Freedom to Maneuver
- Facilitates Monitoring (Can be Watched)
- Offers a Minimum Number of Services
- Is Maintainable (Can be Kept Current)

DON'T MAKE IT EASY – RAISE THE BAR!

[1] Bejtlich, Richard. *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Addison-Wesley, 2010, pp. 20–24.

Reality Bites

- We’re responsible for network security
- Network security is heavily dependent on network architecture
- We don’t usually control network architecture
- We don’t usually get to design the network from scratch

Techniques and Strategies

- Remember that security serves the business
- Don’t get discouraged!
- Get embedded in organizational processes (e.g., technical review board, change control)
- Build relationships with network architects and system admins
- Understand the network architecture and offer concrete suggestions

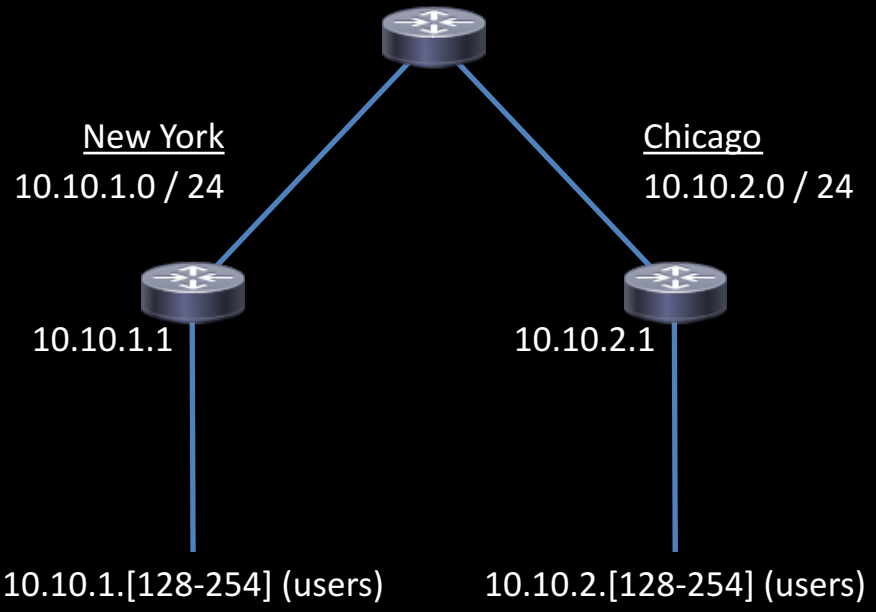
Consistent IP Addressing

- Facilitates Network Administration
- Facilitates Triage / Investigation / Incident Response
- Facilitates Filtering and Monitoring via Firewall Rules and ACLs

Consistent IP Addressing: Example

Remote Offices: 10.10.x.0 / 24

10.10.x.0	:	Subnet
10.10.x.1	:	Gateway
10.10.x.[8-15]	:	Servers
10.10.x.[16-23]	:	Printers
10.10.x.[128-254]	:	Users
10.10.x.255	:	Broadcast



Cisco Wildcard Mask: Basics

- Standard mask

```
/24 = 1111 1111 1111 1111 1111 1111 0000 0000
```

  - 1s = network part of the IP address (i.e., static), 0s = host part (i.e., dynamic)
  - All the 1s are on the left, all the 0s are on the right

- Wildcard mask

```
/24 = 0000 0000 0000 0000 0000 0000 1111 1111
```

  - 0s = static part of the IP address, 1s = dynamic part
  - 1s and 0s can be intermingled

```
10.10.x.50 =  10.10.0.50
              mask 0000 0000 0000 0000 1111 1111 0000 0000
```

  In other words: `10.10.0.50 0.0.255.0`

Cisco Wildcard Mask: Analysis

- We're interested in addresses 10.10.x.[128-254]

```
        10 .         10 .          x .       128 -       254
 0000 1010 .  0000 1010 .  xxxx xxxx .  1000 0000 -  1111 1110
```

- Mask uses 0 for bits that are always the same across all possible addresses; 1 for bits that change

```
 0000 0000 .  0000 0000 .  1111 1111 .  0111 1111
         0 .          0 .        255 .       127
```

Cisco Wildcard Mask: Configuration

Cisco Configuration

```
! Match on 10.10.x.[128-255] -> 10.10.x.[128-255]
access list 101 deny ip
    10.10.0.0 0.0.255.127
    10.10.0.0 0.0.255.127
    log-input
access list 101 permit ip any any

! Apply to the interface facing the user subnet, inbound traffic
interface <interface>
ip access-group 101 in
```

Cisco Wildcard Mask: Application!

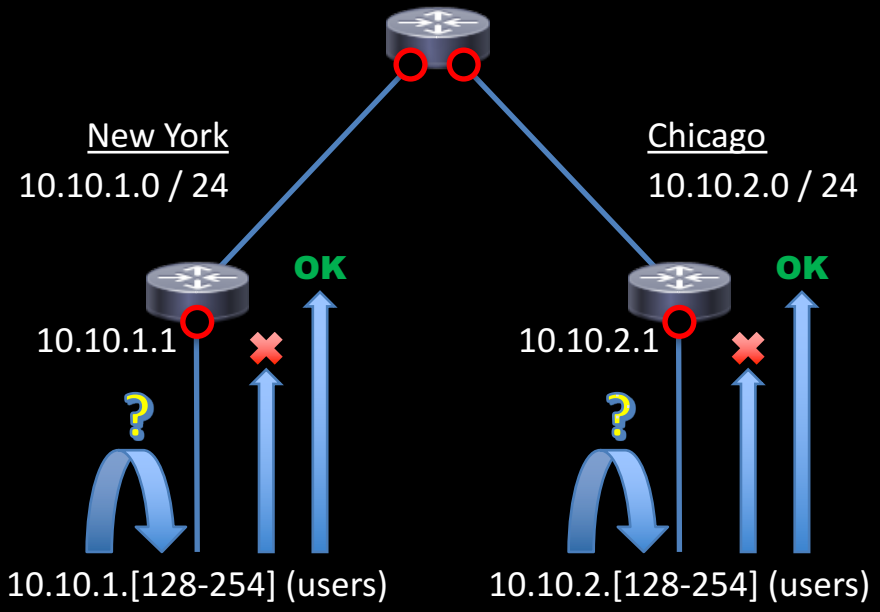
```
access list 101 deny ip 10.10.0.0 0.0.255.127 10.10.0.0 0.0.255.127 log-input
access list 101 permit ip any any
```

- Apply ACL on interface facing user

<u>User -> Remote User</u>
10.10.1.200 -> 10.10.2.200: DENIED!
10.10.2.150 -> 10.10.1.150: DENIED!

<u>User -> Server</u>
10.10.1.200 -> 10.10.2.10: Allowed
10.10.2.150 -> 10.10.1.21: Allowed

<u>User -> Local User</u>
10.10.1.200 -> 10.10.1.150: (not filtered)
10.10.2.150 -> 10.10.2.200: (not filtered)

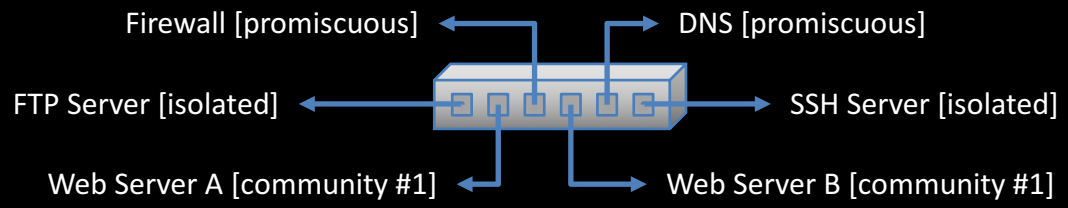


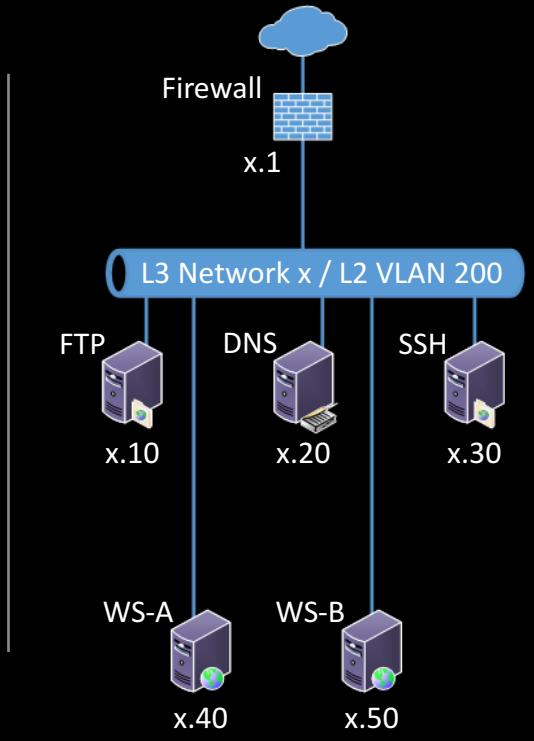
PVLAN: Basics

- PVLAN = Private VLAN
- Further Isolates Traffic Within a VLAN
- Layer 2 (L2) Traffic Control
- Port Types - control communications within the VLAN:
  - Promiscuous: Communicate with any port
  - Isolated: Communicate only with promiscuous ports
  - Community: Communicate with promiscuous ports or ports in the same community

PVLAN: Illustrated Example

Host	PVLAN Port Type	L2 Communications Limited To Ports
Firewall	Promiscuous	All Ports
FTP Server	Isolated	Firewall, DNS
SSH Server	Isolated	Firewall, DNS
DNS Server	Promiscuous	All Ports
Web Server A	Community #1	Firewall, DNS, Web Server B
Web Server B	Community #1	Firewall, DNS, Web Server A





PVLAN: Example – More Details…

- Primary VLAN ID is the VLAN that is being further segregated
- Secondary VLAN IDs identify VLANs to use for isolated and community ports within the primary VLAN

Host	PVLAN Port Type	L2 Communications Limited To Ports	Switch Port	Secondary VLAN ID
Firewall	Promiscuous	All Ports	eth 1/3	n/a
FTP Server	Isolated	Firewall, DNS	eth 1/1	301
SSH Server	Isolated	Firewall, DNS	eth 1/6	301
DNS Server	Promiscuous	All Ports	eth 1/5	n/a
Web Server A	Community #1	Firewall, DNS, Web Server B	eth 1/2	302
Web Server B	Community #1	Firewall, DNS, Web Server A	eth 1/4	302

PVLAN: Example – Config (1 of 3)

Cisco Configuration

```
! Configure VLAN 200 as the primary VLAN so that it can contain individual PVLANs
vlan 200
private-vlan primary

! Configure VLAN 301 as a secondary VLAN: community PVLAN for the web servers using NLB
vlan 301
private-vlan community

! Configure VLAN 302 as a secondary VLAN: isolated PVLAN for the FTP and SSH servers
vlan 302
private-vlan isolated

! Associate the primary VLAN and the secondary VLANs
vlan 200
private-vlan association add 301,302
```

PVLAN: Example – Config (2 of 3)

Cisco Configuration (more…)

```
! Configure the switch ports with the appropriate primary and secondary VLAN associations
interface ethernet 1/1
description FTP server - PVLAN isolated
switchport mode private-vlan host
switchport private-vlan host-association 200 302

interface ethernet 1/2
description Web Server A - PVLAN community #1
switchport mode private-vlan host
switchport private-vlan host-association 200 301

interface ethernet 1/3
description Firewall - PVLAN promiscuous
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 301,302
```

PVLAN: Example – Config (3 of 3)

Cisco Configuration (last bit, I promise…)

```
interface ethernet 1/4
description Web Server B - PVLAN community #1
switchport mode private-vlan host
switchport private-vlan host-association 200 301

interface ethernet 1/5
description DNS - PVLAN promiscuous
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 301,302

interface ethernet 1/6
description SSH server - PVLAN isolated
switchport mode private-vlan host
switchport private-vlan host-association 200 302
```

PVLAN: Application to User Traffic!

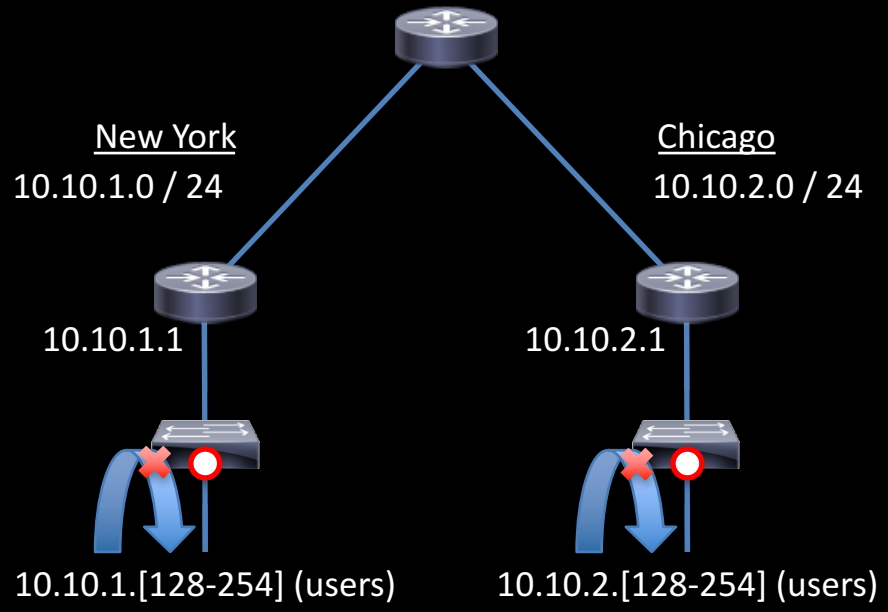
```
vlan 302
private-vlan isolated

vlan 200
private-vlan primary
private-vlan association add 302

interface ethernet 1/1
description router interface
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 302

interface ethernet 1/2-24
switchport mode private-vlan host
switchport private-vlan host-association 200 302
```

- Configure PVLAN on access switches

User -> Local User

10.10.1.200 -> 10.10.1.150: DENIED!

10.10.2.150 -> 10.10.2.200: DENIED!



PVLAN: Fatal Flaw and Easy Fix

Host	IP Address	MAC Address
Router	10.10.1.1	CC:CC:CC:CC:CC:CC
Local User A	10.10.1.100	AA:AA:AA:AA:AA:AA
Local User B	10.10.1.200	???

PVLAN Bypass Packet:

```
10.10.1.100 [AA:AA:AA:AA:AA:AA] ->
10.10.1.200 [CC:CC:CC:CC:CC:CC]
```

- Router happily routes back to local subnet, bypassing PVLAN control
- Easy Fix: VACL or ACL!

```
access list 101 deny ip 10.10.1.0 0.0.0.255 10.10.1.0 0.0.0.255 log-input
access list 101 permit ip any any
```

- BONUS! Already covered by our existing ACL (for the user segment, at least)

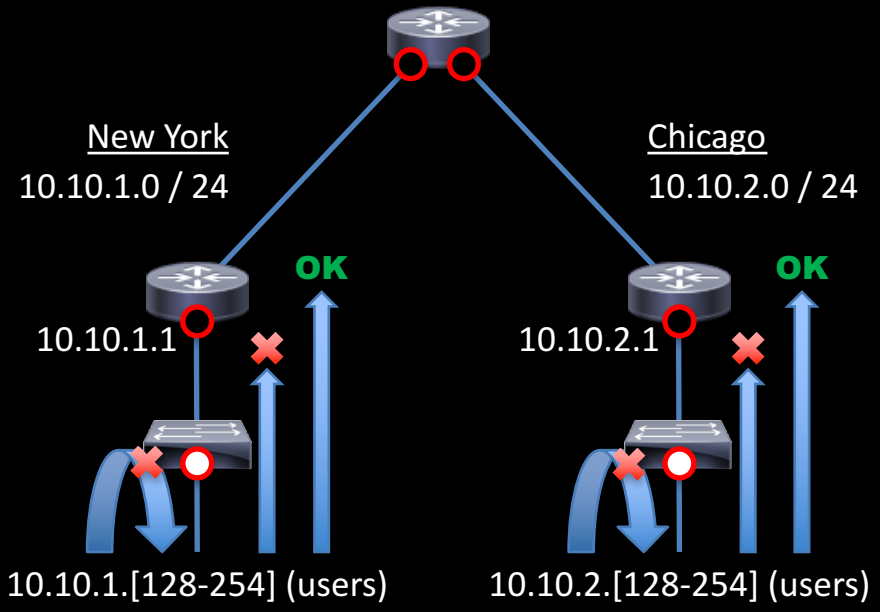
ACL + PVLAN = Block User -> User!

- Apply ACL on interface facing user
- Configure PVLAN on access switches

<u>User -> Remote User</u>
10.10.1.200 -> 10.10.2.200: DENIED
10.10.2.150 -> 10.10.1.150: DENIED

<u>User -> Server</u>
10.10.1.200 -> 10.10.2.10: Allowed
10.10.2.150 -> 10.10.1.21: Allowed

<u>User -> Local User</u>
10.10.1.200 -> 10.10.1.150: DENIED
10.10.2.150 -> 10.10.2.200: DENIED



Wrapping Up

- Build relationships with network architects; participate in their processes
- You can build (or upgrade to) a defensible network
- Remember that every block is an opportunity to detect
- Defend like it's your own network – because it is!

Contact Information

GREG SCHEIDEL

CYBERSECURITY ENGINEER

@greg_scheidel

WWW.IVSEC.COM