Deploying ACLs to Manage Network Security

This Application Note relates to the following Dell PowerConnect™ products:

- PowerConnect 33xx

Abstract

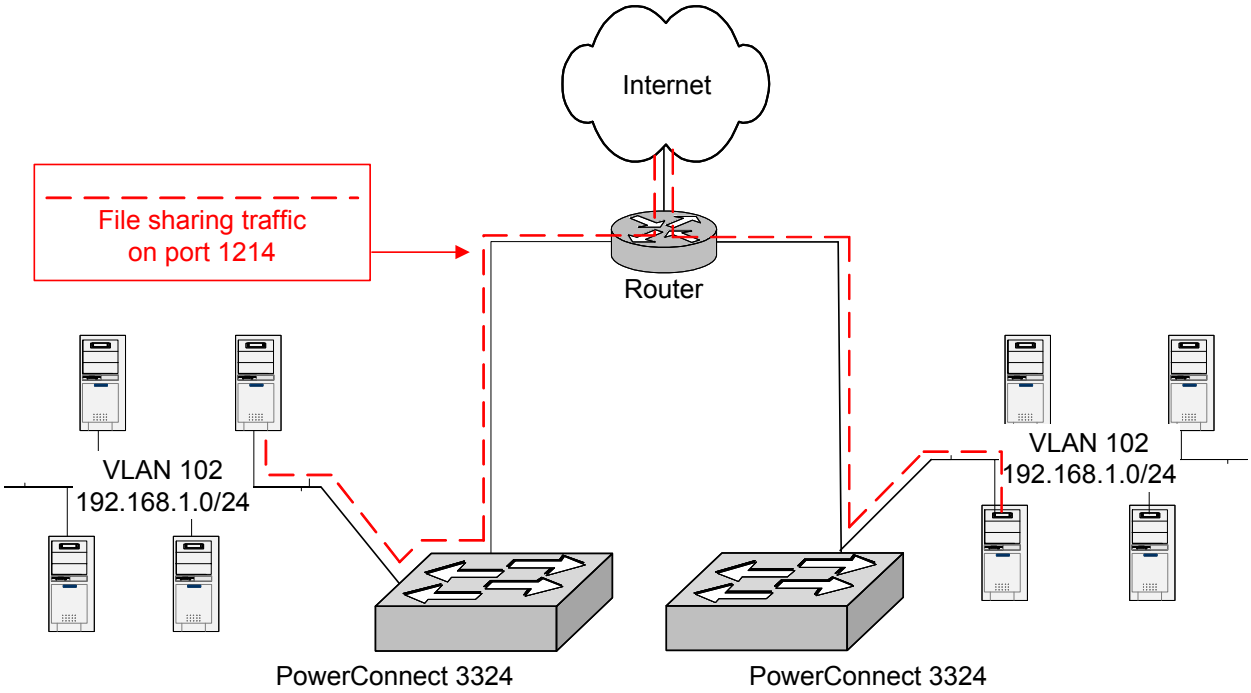
With new system and network vulnerabilities being exposed daily, it is essential for network administrators to develop security policies to protect corporate assets. Dell PowerConnect switches offer flexible access control functions that implement comprehensive security policies. This document explains how to use access control lists (ACLs) to protect various infrastructure elements, including network segments (both physical and logical), network nodes, and applications.

Applicable Network Scenarios

ACLs enhance network and system security by filtering traffic on a per-interface and per-resource basis. Interfaces can include physical Ethernet ports, link aggregation groups (LAGs), and virtual local area networks (VLANs). Resources include network-layer protocols such as IP and GRE, as well as the TCP and UDP ports used by applications.

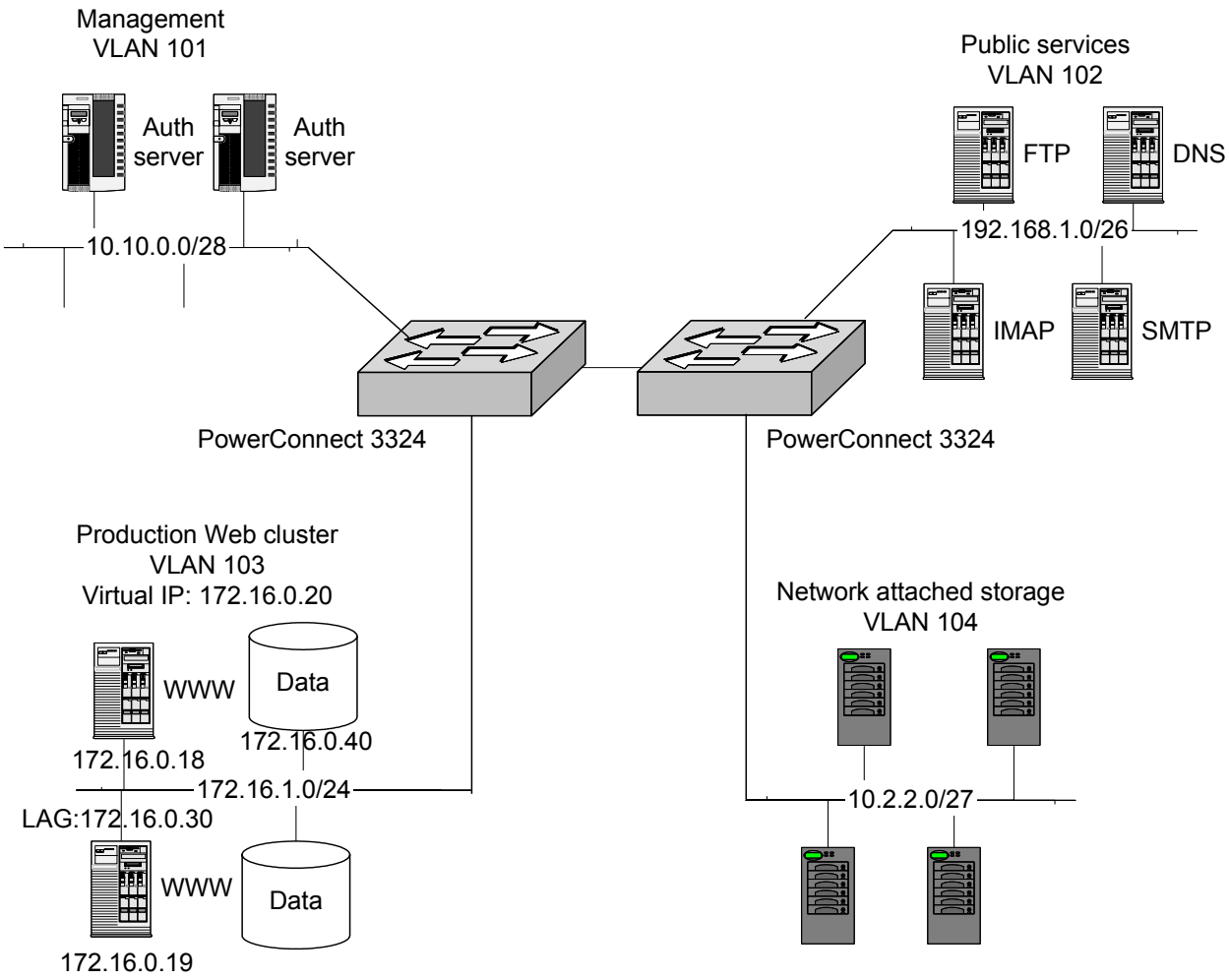
Networks and hosts are substantially more secure with ACLs in place. The following two scenarios offer cases in point.

Scenario 1:
The diagram below depicts a simple network consisting of a single VLAN with no access controls in place to filter out unwanted traffic, such as peer-to-peer file sharing.



With no access controls to block peer to peer traffic, users may overload the network with such traffic. Further, management may be at legal risk if users engage in illegal file sharing.

Scenario 2:
The diagram below depicts an enterprise network comprising various segments, systems, and applications, none of which are currently protected by access controls:



- VLAN 101 provides authentication servers that validate access to network devices and nodes. There are no filters in place to discriminate between traffic sourced from the authentication servers and other traffic.
- VLAN 102 provides public services to the Internet, yet there are no filters to protect it from attack.
- VLAN 103 provides connectivity to a web cluster with a MySQL database and an NFS fileserver. No filters control access to the fileserver or database, leaving them wide open to the rest of the network, including the public services segment.
- VLAN 104 contains network-attached storage (NAS) devices. These systems store sensitive client and enterprise data, but there are no security policies to protect them from the outside world or other internal segments.

Hosts and applications on all four VLANs are vulnerable. Fortunately, ACLs can help enforce a security policy by blocking unwanted traffic.

Technology Background

ACLs provide a logical, intuitive mechanism for defining security policies by grouping various access control entries (ACEs) together to form a set of rules.

A switch processes ACEs in the order they are defined. Thus, a switch compares a frame entering an interface or VLAN against the first ACE defined in an ACL. If the frame matches the criteria of the first ACE, then the switch applies the specified action to the frame. Otherwise, the switch continues to compare the frame to subsequent ACEs.

Since switches process ACEs in order, the most commonly matched conditions should be listed first to minimize processing time. If there is no match in any of the ACEs, the switch will discard the frame. This is considered sound security practice. As a rule, ACLs will block access for all traffic except that for which access is explicitly permitted.

Configurable ACE actions include “permit”, meaning the switch will forward a frame, and “deny”, meaning the switch will discard a frame. Network managers also can use the “disable-port” option with the “deny” action to disable the interface and trigger an SNMP trap notification. The switch will send a trap message after receiving traffic that matches the ACL.

ACLs may be bound to physical interfaces, link aggregation groups (LAGs), and VLANs. Individual ACEs can match against a variety of criteria, including VLAN ID, IP address, source and destination TCP port, and source and destination UDP port. Where quality of service (QOS) enforcement is a consideration, ACEs also can also be mapped to a given diff-serv code point (DSCP) or IP precedence value.

Here is an example of an interface ACL:

```
console> enable
console# configure
console(config)# int ethernet 1/e12
console(config-if)# service-acl input mysql_access
```

The sequence above creates an ACL called “mysql_access” for inbound traffic on interface 1/e12.

Here is an example of a LAG ACL:

```
console> enable
console# configure
console(config)# int port-channel 1
console(config-if)# service-acl input lag_1
```

The sequence above creates an ACL called “lag_1” for inbound traffic on LAG 1 (port-channel 1).

Here is an example of a VLAN ACL:

```
console> enable
console# configure
console(config)# int vlan 104
console(config-if)# service-acl input vlan_104
```

The sequence above creates an ACL called “vlan_104” for inbound traffic on VLAN 104.

It is important to note that ACLs are just one among several defense mechanisms in the security arsenal, including firewalls, virtual private network (VPN) gateways, intrusion detection systems (IDSs), and

others. All these tools have their place. ACLs are an important member of this arsenal because of their ability to keep suspicious traffic from entering the network to begin with.

Proposed Solution

Overview

Scenario 1:

An ACL can be deployed to block peer to peer traffic but permit other traffic.

The following steps can be taken to eliminate peer to peer traffic from the network in Scenario 1.

1. Build ACL that denies all traffic destined for peer to peer services but permits all other traffic.

2. Apply ACL inbound on VLAN 102.

Scenario 2:

ACLs can be deployed to allow only that traffic destined for necessary services required to meet operational goals. Segments that provide connectivity to sensitive data stores should only allow traffic sourced from trusted set of secure hosts.

The following steps can be taken to increase the security of the network in the **Scenario 2.**

1. Apply ACL to VLAN 101 that only permits:
- SSH traffic from any network.

2. Apply ACL to VLAN 102 that only permits:
- Traffic destined for necessary services: DNS, FTP, WWW, and SMTP.
- SSH traffic from management subnet (10.10.0.0/28).

3. Apply ACL to VLAN 103 that only permits:
- HTTP and HTTPS traffic destined for Web server farm (virtual IP: 172.16.1.20).
- SSH traffic from management subnet (10.10.0.0/28).

4. Apply ACL to LAG 1 (attached to Web server 172.16.1.30 in VLAN 103) that only permits:
- NFS traffic from web servers (172.16.1.18 and 172.16.1.19)
- SSH traffic from management subnet (10.10.0.0/28).

5. Apply ACL to interface 1/e12 (attached to database,172.16.1.40, in VLAN 103) that only permits:
- MySQL traffic from web servers (172.16.1.18 and 172.16.1.19)
- SSH traffic from management subnet (10.10.0.0/28)

6. Apply ACL to VLAN 104 that only permits:
- Amanda Backup Services traffic from the database, 172.16.1.40, in VLAN 103
- SSH traffic from management subnet (10.10.0.0/28)

Step-By-Step Instructions

The following configuration guidelines are compatible with Dell PowerConnect 33xx series switches.

SCENARIO 1:

1. Build ACL that denies all peer to peer traffic but permits all other traffic.

```
console> enable
console# config
console(config)# ip access-list vlan_102
console(config-ip-al)# deny-tcp any any any 1214
console(config-ip-al)# permit any any any
console(config-ip-al)# exit
```

2. Apply ACL inbound on VLAN 102.

```
console(config)# int vlan 102
console(config-if)# service-acl input vlan_102
console(config-if)# exit
console(config)# exit
console# copy run start
console# exit
```

WARNING: While this example will block peer to peer traffic, the permit-all ACE may allow other undesirable traffic onto the network. For greater security, define ACEs that permit only authorized applications. The switch will implicitly discard all other traffic once ACLs are invoked.

SCENARIO 2:

1a. Define ACL for VLAN 101 and respective ACEs.

```
console> enable
console# config
console(config)# ip access-list vlan_101
console(config-ip-al)# permit-tcp any any any 10.10.0.0 0.0.0.15 22
```

This ACL permits SSH traffic (TCP port 22) is sourced from any network and destined for the 10.10.0.0/28 management network (VLAN 101). All other traffic is **implicitly denied**.

Note the syntax of the mask in the ACL (0.0.0.255). This is the reverse of the commonly used host subnet mask of 255.255.255.0. In this instance, the ACE masks the *host* part of the IP address, not the network part. Use the following table to determine which masks to use in ACEs:

Subnet mask	Prefix length	ACE mask
255.255.255.0	/24	0.0.0.255
255.255.255.128	/25	0.0.0.127
255.255.255.192	/26	0.0.0.63
255.255.255.224	/27	0.0.0.31
255.255.255.240	/28	0.0.0.15
255.255.255.248	/29	0.0.0.7
255.255.255.252	/30	0.0.0.3
255.255.255.254	/31	unusable
255.255.255.255	/32	0.0.0.0

1b. Apply ACL *vlan_101* to VLAN 101.

```
console(config)# int vlan 101
console(config-if)# service-acl input vlan_101
```

2a. Define ACL for VLAN 102 and respective ACEs.

```
console(config)# ip access-list vlan_102
console(config-ip-al)# permit-tcp any any 192.168.1.0 0.0.0.63 53
console(config-ip-al)# permit-udp any any 192.168.1.0 0.0.0.63 53
```

```
console(config-ip-al)# permit-tcp any any 192.168.1.0 0.0.0.63 21
console(config-ip-al)# permit-tcp any any 192.168.1.0 0.0.0.63 143
console(config-ip-al)# permit-tcp any any 192.168.1.0 0.0.0.63 25
console(config-ip-al)# permit-tcp 10.10.0.0 0.0.0.15 any 192.168.1.0 0.0.0.63
22
```

This ACL permits DNS (TCP and UDP port 53), FTP (TCP port 21), IMAP (TCP port 143), and SMTP (TCP port 25) sourced from any network and destined for 192.168.1.0/26. It also permits SSH traffic (TCP port 22) sourced from 10.10.0.0/28. All other traffic is **implicitly denied.**

2b. Apply ACL *vlan_102* to VLAN 102.

```
console(config)# int vlan 102
console(config-if)# service-acl input vlan_102
```

3a. Define ACL for VLAN 103 and respective ACEs.

```
console(config)# ip access-list vlan_103
console(config-ip-al)# permit-tcp any any 172.16.1.20 0.0.0.0 80
console(config-ip-al)# permit-tcp any any 172.16.1.20 0.0.0.0 443
console(config-ip-al)# permit-tcp 10.10.0.0 0.0.0.15 any 172.16.1.0 0.0.0.255
22
```

3b. Apply ACL *vlan_103* to VLAN 103.

```
console(config)# int vlan 103
console(config-if)# service-acl input vlan_103
```

This ACL permits HTTP and HTTPS traffic (TCP ports 80 and 443, respectively) sourced from any network and destined for the web cluster VIP, 172.16.1.20. It also permits SSH traffic sourced from 10.10.0.0/28. All other traffic is **implicitly denied.**

4a. Define ACL for LAG 1 and respective ACEs.

```
console(config)# ip access-list lag_1
console(config-ip-al)# permit-tcp 172.16.1.18 0.0.0.0 any 172.16.1.30 0.0.0.0
111
console(config-ip-al)# permit-udp 172.16.1.18 0.0.0.0 any 172.16.1.30 0.0.0.0
111
console(config-ip-al)# permit-tcp 172.16.1.18 0.0.0.0 any 172.16.1.30 0.0.0.0
2049
console(config-ip-al)# permit-udp 172.16.1.18 0.0.0.0 any 172.16.1.30 0.0.0.0
2049
console(config-ip-al)# permit-tcp 172.16.1.19 0.0.0.0 any 172.16.1.30 0.0.0.0
111
console(config-ip-al)# permit-udp 172.16.1.19 0.0.0.0 any 172.16.1.30 0.0.0.0
111
console(config-ip-al)# permit-tcp 172.16.1.19 0.0.0.0 any 172.16.1.30 0.0.0.0
2049
console(config-ip-al)# permit-udp 172.16.1.19 0.0.0.0 any 172.16.1.30 0.0.0.0
2049
console(config-ip-al)# permit-tcp 10.10.0.0 0.0.0.15 any 172.16.1.30 0.0.0.0
22
```

This ACL permits NFS traffic (TCP and UDP ports 111 and 2049) sourced from the web servers and destined for the file server. It also permits SSH traffic (TCP port 22) sourced from 10.10.0.0/28. All other traffic is **implicitly denied.**

4b. Apply ACL *lag_1* to LAG 1.

```
console(config)# int port-channel 1
console(config-if)# service-acl input lag_1
```

5a. Define ACL for 1/e12 and respective ACEs.

```
console(config)# ip access-list mysql_access
console(config-ip-al)# permit-tcp 172.16.1.18 0.0.0.0 any 172.16.1.40 0.0.0.0
3306
console(config-ip-al)# permit-udp 172.16.1.18 0.0.0.0 any 172.16.1.40 0.0.0.0
3306
console(config-ip-al)# permit-tcp 172.16.1.19 0.0.0.0 any 172.16.1.40 0.0.0.0
3306
console(config-ip-al)# permit-tcp 10.10.0.0 0.0.0.15 any 172.16.1.40 0.0.0.0
22
```

This ACL permits MySQL traffic sourced from the web servers and destined for the database (MySQL uses TCP and UDP ports 3306). It also permits SSH traffic sourced from 10.10.0.0/28. All other traffic is **implicitly denied.**

5b. Apply ACL *mysql_access* to interface 1/e12.

```
console(config)# int ethernet 1/e12
console(config-if)# service-acl input mysql_access
```

6a. Define ACL for VLAN 104 and respective ACEs.

```
console(config)# ip access-list vlan_104
console(config-ip-al)# permit-tcp 172.16.1.40 0.0.0.0 any 10.2.2.0 0.0.0.31
10080
console(config-ip-al)# permit-tcp 10.10.0.0 0.0.0.15 any 10.2.2.0 0.0.0.31 22
```

This ACL permits Amanda backup traffic (TCP port 10080) sourced from the database and destined for 10.2.2.0/27. It also permits SSH traffic sourced from 10.10.0.0/28. All other traffic is **implicitly denied.**

6b. Apply ACL *vlan_104* to VLAN 104.

```
console(config)# int vlan 104
console(config-if)# service-acl input vlan_104
console(config-if)# exit
console(config)# exit
console# copy run start
console# exit
console>
```

Conclusion

Upon completion of the above configurations, PowerConnect 33xx switches will filter traffic on per-resource and per-host basis.