 **NINJA POSTAL CORPORATION**

**CISCO** white paper

**1**

**EXECUTIVE SUMMARY**

NinjaPostal Corporation, a global organization which specializes in deliveries from Asia to North America. It has engaged our firm to design infrastructure network, which has three in Tokyo (Japan), Toronto and Vancouver (Canada).



The main objective of this project is to communicate with all the three sites by ensuring strong security protocols.

The proposed system includes two Autonomous System (AS), One for Japan and the other is for Canada. An autonomous system is a collection of IP networks that is managed by a single administrative system (Robert, 2021, Para1). Each region has its own AS, ensuring that communication within the AS remains secure.

To protect NinjaPostal’s data, Access Control List (ACL) and Role-Based Access Control are included in the design to improve security. The main purpose of RBAC is for security and authentication (Ron, 2022, Para1). ACL restricts unauthorized users from accessing sensitive and critical data.

In addition to this, NinjaPostal has requested to arrange a small webserver hosted in Tokyo. Which is accessible from Vancouver and only ping requests from Toronto but no access. To deny access and allow ping from Toronto ACLs are configured. Overall security protocols like syslog event violation mode, TFTP servers in Tokyo improve security measures. Our design not only addresses the specific requirements outline but also anticipates future growth and technological advancements.

**CISCO** white paper

**2**

**NETWORK TOPOLOGY**

A diagram of a diagram

Description automatically generated

**CISCO** white paper

**3**

**DESIGN JUSTIFICATION AND OVERVIEW**

**Routing Protocol:**

EIGRP and BGP: We implement EIGRP for efficient intra-office routing within each AS, while BGP handles optimal inter-office routing across AS systems.

**A computer screen with icons

Description automatically generated with medium confidenceJustification:** EIGRP ensures rapid intra-office communication, while BGP offers precise control over inter-office traffic routing.

**Benefits:** Fast Convergence: EIGRP ensures quick intra-office communication.

Optimal Routing**:** BGP's path selection and policy-based routing enhance inter-office traffic efficiency.

Redundancy: Both protocols provide failover for uninterrupted communication.

**VLAN Implementation:**

**Justification:** VLANs segment network traffic logically, improving performance and security.

**Benefits:** Security and Isolation: VLANs isolate Admin and General users, enhancing security.

Bandwidth Efficiency**:** VLAN segmentation optimizes bandwidth usage.

Simplified Management**:** V Lans streamlines troubleshooting and management.

**ACLs and RBAC:**

**Justification:** ACLs and RBAC bolster network security by controlling access to resources and devices.

**Benefits:** Enhanced Security: ACLs restrict access to the Tokyo web server, mitigating unauthorized access risks.

Access Control**:** RBAC ensures precise access levels for administrators, minimizing privilege escalation.

Comprehensive Security**:** ACLs and RBAC form a robust security framework, safeguarding against unauthorized access and internal threats.

BGP: We implement EIGRP for efficient intra-office routing within each AS, while **CISCO** white paper

**4**

BGP handles optimal inter-office routing across AS systems.

**IP CONFIGURATION MATRIX:**

A table with different colored lines

Description automatically generated with medium confidence

**CISCO** white paper

**5**

**SECURITY AND COMPLIANCE OVERVIEW**

**ACLs:**

**Purpose**: It controls traffic flow and restricts access to network resources (Chidiadi, 2023, Para 2).

|  |
| --- |
|  |

**Implementation**:

* Permits traffic from Admin VLAN in Vancouver to Tokyo web server.
* Denies traffic from General VLANs to Admin VLANs.
* Restricts access to management interfaces based on RBAC roles.

**RBAC:**

**Purpose:**

* It has control over user access to critical network devices (Abi, 2023, Para 1).
* It limits the access to the users to certain access to data on the network based on their role within the organization.
* This helps to control who has access to sensitive information while also keeping that information secure.
* For a successful implementation of access control, it should fulfil the segments such as identification, authentication, and authorization.

**CISCO** white paper

**6**

**Implementation:**

* It has three distinct user roles with specific permissions: Admin, Network Operator, Helpdesk. Admins have full access, Network Operators can modify configurations, and Helpdesk has limited read-only access.
* A computer network diagram with colorful lines

  Description automatically generatedAccess can be granted or denied based on the ACL.

**Port-Security and Syslog:**

**Purpose:**

* It prevents unauthorized device connections and centralizes logging for monitoring.
* The log file is useful to an Administrator when troubleshooting problems with the device because they can see all the events which took place at a certain time, date, and zone (Harris, n.d., Para 13).

**Implementation:**

* The Port-Security limits each port to one connected device.
* Syslog events are sent to the centralized server in Tokyo for auditing and troubleshooting.

**TFTP Server:**

**Purpose**: It Centralizes location for device configuration backups and updates.

**Security Measures:**

* Access restricted based on RBAC roles.
* Regularly updated passwords and secure file transfer protocols implemented (John, 2022, Para 14).
* Limited access to TFTP server from specific management VLANs only.
* Regular monitoring and auditing of TFTP server activity logs.
* **CISCO** white paper

**7**

**FUTUREPROOFING AND SCALABILITY**



Ninja Postal Corporation proposed network design promotes future growth by meeting companies present requirement.

**Scalability:**

Organization growth can be promoted by adding new VLANs and this can help to extend the offices in new places.

**Redundancy:**

To reduce the results of hardware failures, redundant hardware components are implemented to ensure the network is available all the time. So that, if one network connection fails then automatically it connects to secondary connection (C Duron, 2023, Para 4).

**Dynamic Routing Protocol:**

Use of dynamic routing protocols such as EIGRP and BGP allows easy integration and flexibility to the new technologies in the network topology.

Security Measures: Implementation of RBAC and ACL are designed for security improvements. As the organization increases in future, the security measures are adjusted according to the requirements.

Overall, our proposed network design for NinjaPostal Corporation satisfies the needs of secure and scalable communication between its offices in Tokyo, Toronto, and Vancouver. Security, performance, and ease of management are secured by implementing the use of VLANs, dynamic routing protocols, ACLs, RBAC, and centralized services like the TFTP server. These will help for future growth and technological innovations.

**8**

**CISCO** white paper

**REFERENCES**

* Robert Sheldon (2021, August) *autonomous system (AS)*

<https://www.techtarget.com/searchnetworking/definition/autonomous-system>

* Ron A (2022, October 6) *What are Role-Based Access Control (RBAC) and ACL (Access Control Lists) and how are they used?*

<https://ron-a.medium.com/what-are-role-based-access-control-rbac-and-acl-access-control-lists-and-how-are-they-used-e8d26a74c0a1>

* Chidiadi Anyanwu (2023, April 14) *What is an ACL? Access Control Lists Explained*

<https://www.freecodecamp.org/news/a-deep-dive-into-access-control-lists/>

* Abi Tyas Tunggal (2023, Apil 20) *What is Role-Based Access Control (RBAC)? Examples, Benefits, and More*

<https://www.upguard.com/blog/rbac>

* Harris Andrea (n.d.) *All About Syslog Protocol (What is Syslog, Default Port, Purpose etc)*

<https://www.networkstraining.com/all-about-syslog-protocol/>

* John Carl Villanueva *(2022, December 11) What is TFTP? | Trivial File Transfer Protocol*

<https://www.jscape.com/blog/what-is-tftp>

* C Duron (2023, November 15) *Futureproofing: Planning Networks for Scalability*

<https://www.techrecur.com/futureproofing-planning-networks-for-scalability/>

**9**

**CISCO** white paper