PROJETS PROFESSIONNELS ETUDIANTS

LICENCE, MASTER & CERTIFICATS PROFESSIONNELS CYCLE LONG

**ARCHITECTURE DE LA SOLUTION**



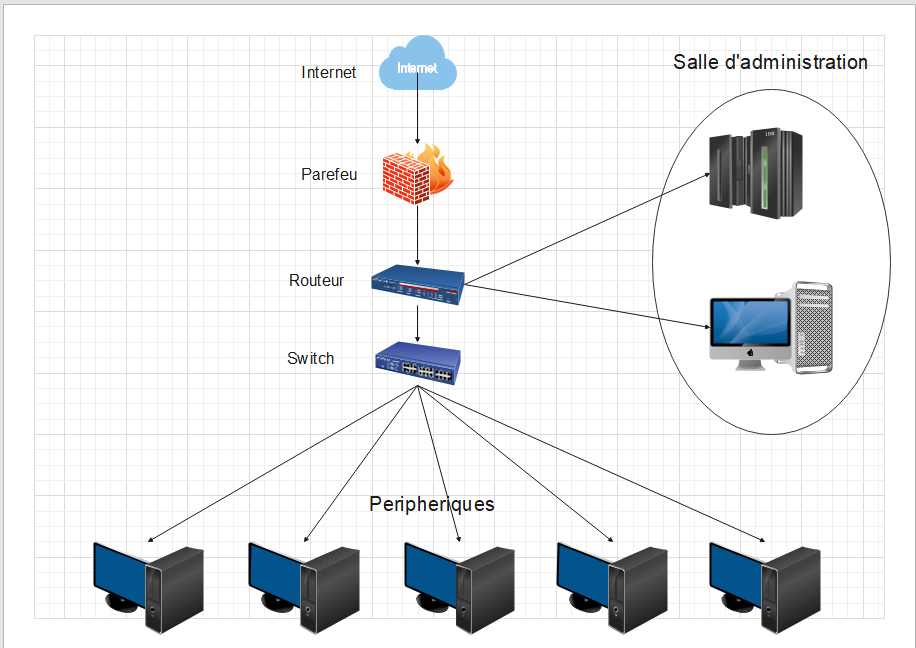
**Membres du groupe** : **Encadreur :**

**Elisée DATE-MASSE**

**Wealth Josias KATCHE**

**Amos Kokou KOUGBLENOU**

**Essolizam KEZIE**

****

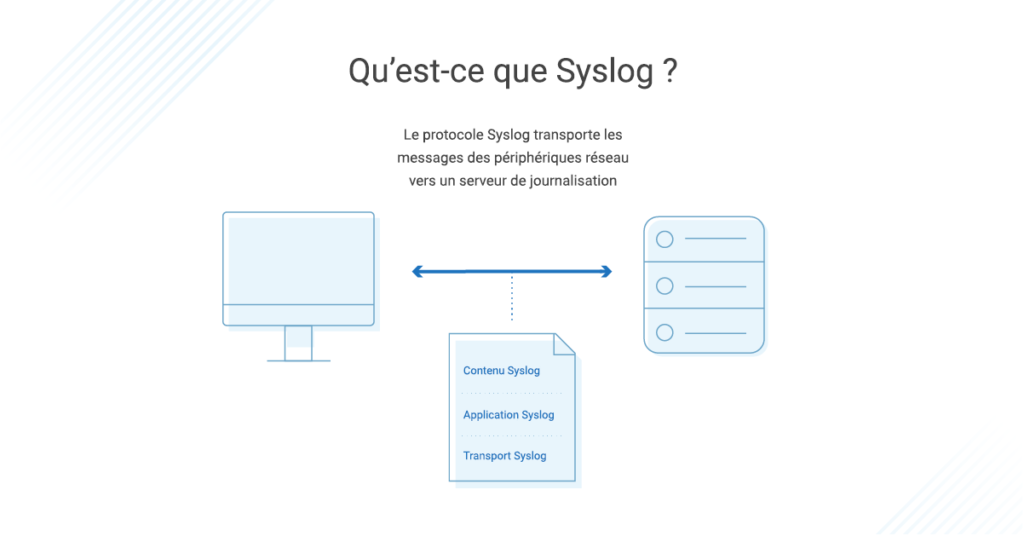
**DESCRIPTION DE L’ARCHITECTURE**

L’architecture Network Performance Monitoring est basée sur des agents, s’exécutant sur les points de terminaisons surveillés, qui transfert les données de sécurité à une centrale serveur où sont centralisée les évènements. De plus les périphériques sans agents (tels que les pares-feux, les commutateurs, les routeurs, les points d’accès etc..) sont pris en charges et peuvent soumettre activement des données de journal via Syslog, ssh, ou à l’aide leur propre API.

Le diagramme ci-dessus représente une architecture de déploiement de Network Performance Monitoring with Syslog and SNMP. Il montre les composants de la solution (Dans notre cas deux serveurs Windows tournant sur Windows Server Datacenter 2016, une machine Windows 10 et des machines cibles tournant sur une quelconque version de Windows) et comment le serveur dédié Syslog et PRTG peuvent être configurés en tant que hôtes, offrant un équilibrage de charge et de haute disponibilité.

**AGENT SYSLOG - COMMUNICATION DU SERVEUR SYSLOG**

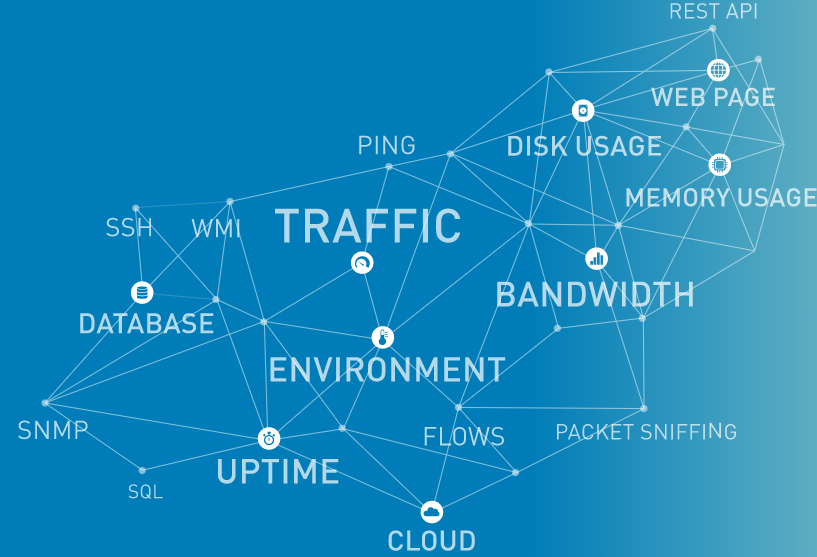
Les périphériques réseau tels que les serveurs, pare-feux et routeurs génèrent des journaux sur les événements et les statuts, et il peut être difficile de suivre toutes ces informations. Avec l’agent Syslog, associé à un serveur Syslog tel que Kiwi Syslog nous pouvons facilement gérer et consulter tous ces journaux.



**AGENT SNMP - COMMUNICATION DU SERVEUR PRTG**

Le serveur PRTG utlise l’agent SNMP pour superviser l'ensemble du système, appareils et applications de notre infrastructure informatique.

L’interface utilisateur web de PRTG permet de créer des capteurs ou sondes en s’appuyant notamment sur l’ICMP, le SNMP...afin d’afficher les informations relatives à la configuration et à l’état des équipements du parc informatique. L’administrateur peut également modifier, via des appels d’API, des agents ou des paramètres de configurations de serveur lorsque vous le souhaitez. Cette communication est cryptée avec TLS et authentifiée avec un nom utilisateur et un mot de passe.



**PORTS REQUIS**

Pour la communication des composants du Network Performance Monitoring with Syslog and SNMP, plusieurs services sont utilisés. Nous essayerons d’énumérer ci-dessous la liste des ports par défauts utilisés par ses services. Les utilisateurs peuvent modifier ces numéros de ports si nécessaire.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Component** | **Software** | **Port** | **Protocol** | **Purpose** |
| Syslog Server | Kiwi Syslog | 514 | UDP | Utiliser pour les messages Syslog |
| 22 | TCP | Utiliser pour un accès Shell securisé |
| 80 | HTTP | Accès web |
| PRTG Server | PRTG | 161 | SNMP-UDP | Envoie des traps SNMP |
| 162 | SNMP-UDP | Reception des traps SNMP |
| 135 | WMI-TCP |  |
| 25 | SMTP-TCP | Utiliser pour les mails |
| 443 | SSL | Accès web securisé |
| 80 | HTTP | Accès web |