University of Colorado
Interdisciplinary Telecommunications Program TLEN 5700

Securing the CU Boulder Enterprise Network with Flow-Based Analysis
Concept Definition Document (CDD)

10/26/2017

1.0 PROJECT INFORMATION

Project Customers

| Name: CU - Boulder IT/Security Team (Joe McManus) Address: 1045 18th St, Boulder, CO Phone: 303-735-4357 Email: help@colorado.edu | Name: Address: Phone: Email: |

Team Members

<table>
<thead>
<tr>
<th>Name: Erin Simons-Brown Phone: (720) 308-3448 Email: <a href="mailto:Erin.Simons-Brown@colorado.edu">Erin.Simons-Brown@colorado.edu</a></th>
<th>Name: Jacob Levine Phone: (303) 378-8765 Email: <a href="mailto:jale6295@colorado.edu">jale6295@colorado.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Paxaj Shukla Phone: (720) 755-7817 Email: <a href="mailto:pash8888@colorado.edu">pash8888@colorado.edu</a></td>
<td>Name: Phone: Email:</td>
</tr>
</tbody>
</table>
2.0 Project Description

The University of Colorado - Boulder (CU) is a large campus and has a large and complex network. Because of this, CU’s network is subject to frequent cyber attacks. The university currently monitors all network traffic using QRadar as their security information and event monitoring (SIEM) system.

According to CU’s IT Security Office (ITSO), QRadar generates 85 million of alerts per day. Only a small fraction of these alerts are true security concerns, and CU’s small IT security team does not have the time or the manpower to wade through them all.

The purpose of the project is to build a better network monitoring system for CU IT security. One that can perform initial triage, provide focused alerts, and filter out more noise. The system will use network flow-based traffic analysis that allows users to detect threats and intrusions while maintaining the privacy of the network users.

The project objectives are specified below:

**Level 1:**
Deployment of the Cisco Stealthwatch on at least 20 data sources. These data sources will be located on and around the University of Colorado - Boulder campus.

**Level 2:**
Analyze the data and produce actionable security info. “Actionable security info” here means information that can be utilized by CU’s IT security office to improve campus network security in the following ways:
1. Detect breaches and insider threats faster
2. Accelerate analysis and understanding of incidents
3. Identify/target data hoarding
4. Enable deployment of software-based segmentation/security policy
5. Quarantine compromised user to control breach & remediate breach

**Level 3:**
Create a cost analysis of the new Cisco-based system vs. the current system that CU uses (QRadar). This analysis will include not only direct financial costs incurred by both systems, but also indirect costs such as time spent configuring each tool, percentage of overall employee time spent on each tool, and the likelihood of each tool to correctly alert CU ITSO of potential attacks.

**Level 4:**
User testing will begin. This will primarily consist of using first year Interdisciplinary Telecommunications Students (ITP) as the test users. These users will generate security reports based on the newly implemented system. After using the system, the users will provide feedback on aspects such as ease of use, simplicity of design, and how difficult real threats are to detect.
Concept of Operations:

Figure 1. Concept of Operations Diagram (CONOPS)

Figure 2. Functional Diagram
Functional Requirements:

This project is essentially a scalable version of what CU will implement campus-wide. Thus, this 20-node project will be self-contained, and will act as a proof-of-concept to the CU ITSO for implementing the Cisco services on the CU network.

Technical:

CPE 1.1 Install and configure required appliances. In order to capture network flow data, it is necessary to install and configure the Cisco Stealthwatch Flow Collector and the Cisco Stealthwatch Management Console appliances.

CPE 1.2 Devise an analyzation technique. Compose a plan for analyzing the data in order to produce actionable results. The method for analysis may need to be adapted as the project progresses in order to improve results.

CPE 1.3 Develop a test plan for user tests. Create test plans to use for our user tests. These test plans will help in evaluating things such as ease of use, quality of data generated, and any problems encountered.

Logistical:

CPE 2.1 Identify at least 20 data sources. In order to achieve the base-level objectives, a minimum of 20 data sources around the campus are needed to collect network traffic flow.

CPE 2.2 Gather cost and operation information. Obtain as much information as possible about the cost of the current system, as well as the cost of the new system. The campus IT security can provide the information regarding the cost of the current system, and the Cisco contact can provide the information regarding the new system.

CPE 2.3 Coordinate between CU ITSO’s needs and Cisco’s platform. The CU security team’s demands must be met, while ensuring that those demands are met by using Cisco’s security platform. If any conflicts arise, they should be clearly communicated to both parties.

Financial:

There are no critical financial elements involved as of now. The CU ITSO already has licences in place for the Cisco equipments. In addition, Cisco has indicated their willingness to loan extra equipment to the project on a short-term basis.
3.0 Design Requirements

Functional (FNC.X) as well as the design requirements (DES.X.X) for the project are specified below:

**FNC.1** The project shall have sufficient breadth and depth to provide CU with a sufficient proof-of-concept.

**DES.1.1** The system shall collect data from a minimum of 20 data sources.
**DES.1.2** The system shall be scalable to a size appropriate to monitor the entire campus internetwork.
**DES.1.3** The project shall provide enough data to normalize behavior.
**DES.1.4** The project shall provide enough data to detect unusual behavior.
**DES.1.5** The project shall provide enough data to analyze the effective breadth and depth of the Indicators of Compromise.
**DES.1.6** The system shall use Cisco’s security platforms.
**DES.1.7** The system shall monitor CU’s network traffic.

**FNC.2** The system shall produce actionable and meaningful security threat information.

**DES.2.1** The system shall perform initial triage on the data.
**DES.2.2** The system shall provide focused alerts that filter out more of the noise and generate few, more accurate alerts than the current system.
**DES.2.3** The system shall be configurable to meet CU’s needs.
  **DES.2.3.1** The system shall allow for designing CU ITSO’s security policies.
  **DES.2.3.2** The system shall allow for enforcing CU ITSO’s security policies.

**FNC.3** The project shall provide meaningful information to the CU ITSO in terms of comparison to their current security platform.

**DES.3.1** The system shall contain a log of the previous 18 month’s worth of activity.
**DES.3.2** The system shall meet the current requirements of the current security platform used by CU ITSO.

4.0 Key Design Options Considered: Flow Monitoring and Analysis

**Juniper Flow Monitoring and Analysis**

Juniper Networks offer several options for capturing and analyzing the network flow data. For example, Juniper offers flow monitoring on its M, MX, and T series routers. Juniper offers both active and passive monitoring on these routers, where active means that the
router is part of the network, receiving and forwarding packets, and passive monitoring means that the router is only receiving traffic [1].

Outgoing flow data can be encrypted or tunneled [1], and there are three possible output formats for the data: version 5, version 8, and version 9. Passive data is only available in version 5. Version availability depends on your specific Juniper hardware and Junos OS version. The type of data collected consists of [4]:

- Source and destination IP address
- Total number of bytes and packets sent
- Start and end times of the data flow
- Source and destination port numbers
- TCP flags
- IP protocol and IP type of service
- Originating AS of source and destination address
- Source and destination address prefix mask lengths
- Next-hop router’s IP address
- MPLS label (version 9 only)
➢ ICMP (version 9 only)

Another example is Juniper’s Network Director, available on it’s JA2500 platform. Network Director can perform flow analysis using Juniper’s Cloud Analytics Engine [5]. Network Director uses Network Traffic Analysis to monitor the network, sending data to the data learning engine (DLE), which is part of the Cloud Analytics Engine. The Cloud Analytics Engine analyzes the data in order to improve performance and availability.

Table 1. Pros and Cons of Juniper

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generates flows with configurable parameters.</td>
<td>Analyzation of flows not available for all Juniper devices.</td>
</tr>
<tr>
<td>Flow analysis can improve network performance and availability.</td>
<td>Not tailored towards improving security specifically. Focus is more on application flow through the network.</td>
</tr>
<tr>
<td>High scalability.</td>
<td>Complex configuration and setup.</td>
</tr>
</tbody>
</table>

CA Network Flow Analysis

CA Network Flow Analyzer (NFA) is a proprietary software that collects flow from various routers in a network infrastructure, and provides analysis to aid network visibility [6]. An important distinction here is that the CA NFA does not generate flows like Cisco equipments do, it merely provides analysis of the flow data.

The CA NFA functions in four simple steps: data collection, data aggregation, data storage, and reporting. In the first step, flow data is collected from different vantage points via SNMP. Next, the collected data is “aggregated” or normalized. This is the step where most of the processing occurs and the performance data is obtained. Following data aggregation, the processed output is stored in a database or a “repository”. Finally, the output is sent to the “performance center”, which is a GUI and presented in a dashboard for monitoring. A great flow diagram from the CA NFA’s website is presented in Figure 5.

The CA NFA provides smart in-built capabilities such as classifying and prioritizing different activities and establishing traffic patterns. Moreover, it is scalable, works out of a single collection and aggregation point and ships with a simple and easy-to-use GUI [8]. However, it will suit the project’s needs only if the routers support flow data. Additionally, there are not a lot of APIs for configuration. In a dynamic environment, making configuration changes would require time and effort, which will be a challenge especially in a small team like the ITSO.
Table 2: Pros and Cons of CA NFS

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central data collection and aggregation point, would save money and</td>
<td>Does not generate flows, merely analyzes it.</td>
</tr>
<tr>
<td>space.</td>
<td></td>
</tr>
<tr>
<td>A pre-configured out-of-the-box system, easy to implement.</td>
<td>Little to no APIs, difficult to configure to dynamically changing</td>
</tr>
<tr>
<td></td>
<td>needs.</td>
</tr>
<tr>
<td>Easy-to-use GUI, makes troubleshooting simpler.</td>
<td>No support center in Boulder. Support would not be quick compared to</td>
</tr>
<tr>
<td></td>
<td>Cisco.</td>
</tr>
</tbody>
</table>
Cisco combines Stealthwatch with their Identity Services Engine (ISE) in order to create a NetFlow-based security platform. The process requires that all Cisco routers, switches and firewalls on the network are enabled to capture NetFlow, which then is processed by ISE and Stealthwatch. While many security platforms only monitor the edge of the network, Stealthwatch “delivers comprehensive visibility at the network core, edge, data center and cloud” [9]. Because of this, Stealthwatch can monitor internal threat actors, which oftentimes pose a great risk than external threats. In addition, the combination of Stealthwatch and ISE can give the security team more information on the behavior and identity of the network traffic by “including user name, device type, location, the services being used, and when and how the device accessed the network” [9].

The Stealthwatch platform is based on three main components: the Flow Rate License, the Flow Collector, and the Management Console [11]. In addition to being required to facilitate data collection, the Flow Rate License also dictates the amount of flow that may be collected in terms of flows-per-second (fps). The Flow Collector gathers flow telemetry from NetFlow. It can store up to several months worth of flow data, and a system can handle up to 240,000 fps, depending on the hardware used [11]. The Management Console “aggregates, organizes and presents analysis” [11] on the flow telemetry collected by a Flow Collector. It can data from up to 25 Flow Collectors, in addition to data from ISE. Is is easy to scale up for larger networks and comes in the form of either a Physical Appliance, or a Virtual Edition [11].

In addition, enterprises may choose to purchase the Cisco Stealthwatch Endpoint License which allows the security team to have more visibility over end-users [12], especially mobile ones. On any given day, tens of thousands of CU students, staff and faculty are actively moving around the campus with their cell phones connected to the network. Because of this, CU might want to consider this license if they haven’t already done so.
Table 3. Pros and Cons of Cisco Stealthwatch

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>CU has already purchased most of the licenses required.</td>
<td>Requires use of two Cisco platforms (Stealthwatch and ISE)</td>
</tr>
<tr>
<td>Local Cisco office would provide support in setting equipment up.</td>
<td>Requires network nodes to be Cisco-based</td>
</tr>
<tr>
<td>High scalability</td>
<td></td>
</tr>
<tr>
<td>Designed to monitor entire network for security threats</td>
<td></td>
</tr>
</tbody>
</table>

5.0 Trade Study Process and Results

Table 4: Trade Study Parameters, Weights and Reasoning

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Weight</th>
<th>Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>The project is serving as a proof-of-concept for implementing a new security platform on CU’s network. Given the size of CU’s network, it is extremely important that whichever platform is chosen is easily scalable to a much larger network than just 20 nodes.</td>
<td>.3</td>
<td>5 - Indicates high scalability 1- Indicates low scalability</td>
</tr>
<tr>
<td>Flexibility/Configurability</td>
<td>One of the issues faced with the current security platform is the sheer volume of data being collected and displayed to the user. The new platform must be easily configured to triage alerts and events such that the security team is only notified when a high-level threat is detected.</td>
<td>.2</td>
<td>5 - Indicates high flexibility/configurability 1- Indicates low flexibility/configurability</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Because CU’s network is so large, it is important that the platform chosen is works well with cross-platform systems. CU has many data points, and not all of them will necessarily be the same vendor or the most up-to-date technology. Therefore, it is important that the security platform can play well with other equipment.</td>
<td>.1</td>
<td>5 - Indicates high compatibility 1 - Indicates low compatibility</td>
</tr>
<tr>
<td>Cost</td>
<td>While cost is a major issue in most cases, in this particular project it holds less weight than usual. CU has already purchased most of the licenses needed to implement Cisco’s security platform, but they are waiting to buy the last license needed. Therefore cost is still an important</td>
<td>.1</td>
<td>5 - Indicates low cost 1 - Indicates high cost</td>
</tr>
</tbody>
</table>
factor to look at, but it is by no means the deciding factor when determining which product is the best.

### Time to Deploy
It is imperative that the security platform used by CU takes minimal time to deploy. It can be assumed that deployment would include a brief down-time during which some or all of the network is not being monitored. Given the high amount of activity on the network at any given time, down-time for the monitoring system should be kept to a minimum in order to reduce the likelihood of an attack going unnoticed.

### Maintenance
The CU ITSO is a small team and almost always has a large number of tickets to follow up. Consequently, the ITSO should prefer not to spend too much time maintaining the system.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Weight</th>
<th>Juniper</th>
<th>CA Network</th>
<th>Cisco</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>.3</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Configurability</td>
<td>.2</td>
<td>3</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Compatibility</td>
<td>.1</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Cost</td>
<td>.1</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Time to Deploy</td>
<td>.2</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Maintenance</td>
<td>.1</td>
<td>4</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1</td>
<td>3.2</td>
<td>3.9</td>
<td>4.5</td>
</tr>
</tbody>
</table>

### 6.0 Selection of Baseline Design
While Juniper equipments support netflow generation and aggregation, it is still in its nascent stages. Juniper neither provides analysis tools for the aggregated net flow, nor APIs for configuring flows. Moreover, the current facilities available in the Juniper netflow are geared more towards network performance monitoring and less towards security. On the other hand, Cisco have been the forerunners of net flow analysis. All of the Cisco devices support netflow generation out of the box, and aggregating and analyzing the generated
flow is very simple in the Cisco devices. Moreover, Cisco provides a variety of APIs to configure the flow analysis suited to the project’s needs.

Although the CA NFA has a lot of great features such as establishing and classifying traffic patterns, the Cisco proprietary software is a good fit as it already has most of the capabilities of the CA NFA. Moreover, there are active licenses in place. Consequently, implementing, configuring and maintaining the Cisco proprietary software on Cisco hardware is very simple owing to a variety of REST APIs and abundant documentation. Most importantly, since Cisco is already actively involved with the CU ITSO, support should not be difficult to come by.

Additionally, because scalability is one of the main concerns of the project, it is important to compare the scalability of each option. In doing so, Cisco Stealthwatch becomes the favorite among the three, since it appears to scale the easiest. Somewhat related is the fact that CU’s network is heavily composed of Cisco equipments, so implementing a Cisco-based platform lends itself to being the most simple and effective solution.

Following the arguments made above, it can be concluded that the Cisco proprietary softwares and hardwares suit every requirement of the project.

7.0 References


