Securing a K-12 School Network with a Palo Alto Firewall

Greg Bolek

Lewis University

ABSTRACT

Technology use in schools continues to grow. As schools strive to create 21st Century Learning environments, conduct online testing, or implement BYOD or 1:1 initiatives, it is important that their networks be properly secured. The ultimate goal for a school district is to be able to guarantee network access when it is needed. Without proper visibility into network traffic, this goal becomes impossible. With the growing landscape of applications available, it is important to understand the fundamental differences in how firewalls work and why older generation firewalls simply cannot protect networks effectively anymore. Next-Generation firewalls and their ability to inspect Application Layer traffic is necessary. Palo Alto Networks is a leader in Next-Generation enterprise firewalls. The three core technologies of Palo Alto Networks firewalls - App-ID, User-ID and Content-ID - can be used to solve common problems within a school network.

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

As school districts continue to move forward with technology initiatives, network administrators are tasked with "making it all work." Whether the technology is used to create 21st century learning environments, implement online testing, or support BYOD (Bring Your Own Device) or 1:1 programs, network administrators have to ensure the security of their network. This includes protecting it from threats, ensuring its availability and maintaining compliance with the law. School districts are not immune to attacks that can impact instruction, disrupt online assessments or expose private student information [1]. They also have legal responsibilities to protect children from harmful content [2]. Ultimately, school network administrators can better secure their network if their firewall has visibility into the traffic on their network.

1.1 21st Century Learning Environments

The Department of Education's National Educational Technology Plan published in 2010 recommends schools provide broadband access to the Internet, provide adequate wireless connectivity in school, and provide every student and educator have at least one Internet accessible device [3]. While these goals may seem ambitious, many school districts continue to move forward and adopt technology to support learning and instruction in their classrooms. Whether it is a traditional computer lab approach, high availability environments with carts of laptops or tablets, or 1:1 programs, technology continues to change the way students learn. These 21st century learners have access to a world of information at their fingertips [4]. As technology continues to influence our students and impact instruction in the classroom, school districts also are utilizing technology in the administration of online assessments.

1.2 Online Assessments

As Illinois schools prepare for the PARCC common core assessment, many will be required to administer the assessment online. The Partnership for Assessment of Readiness for College and Careers (PARCC) is one of two multi-state consortia that received $350 million in federal funds to develop new tests aligned with the "Common Core" curriculum standards [5]. The state has recently finished collecting data to determine the districts that will test online and the first PARCC tests will be administered in early Spring of 2015. School districts that meet bandwidth and device requirements will be selected to administer the PARCC assessment online for grades three through eight. However, state assessments are not the only online testing schools are doing. Many districts utilize online testing for local assessment data and in classroom instruction. Companies such as NWEA and Renaissance Learning have popular testing platforms widely used by schools. The improved data collection, increased data accuracy and accessibility features that accompany online testing make it extremely beneficial for schools [6]. Testing online, however, has its impact on the network. Many schools wish to administer tests as quickly as possible, keeping the testing window small. This can only be accomplished by testing large numbers of students at once. Consequently, due to the amount of devices being utilized for testing, schools must be able to control the traffic on their network.

1.3 BYOD and 1:1 Initiatives

With the proliferation of low-cost devices, such as iPads, Chromebooks and similar alternatives, BYOD (Bring Your Own Device) and 1:1 initiatives have become increasingly common in K-12 school districts. Implementation of bring-your-own-device (BYOD) programs in school districts has exploded since last year, spreading from 22 percent to 56 percent [7]. As schools continue to add devices on their networks, school IT leaders must ensure the security and capacity of their networks [8].

1.4 Legal Responsibilities

There are several federal laws schools must follow to protect students. The most important is CIPA, the Children's Internet Protection Act. Enacted in 2000, it states that schools receiving federal E-Rate funds must filter Internet traffic to prevent access to obscene or harmful content [2]. Consequently, school districts generally filter content either through software or hardware solutions. Software solutions have been around for years such as Squid, Untangle and Dansgaurdian. Consequently, firewall companies have begun to integrate content filtering within their products making them more attractive to education customers.

1.5 Summary

As school districts continue to adopt new technologies, school network administrators are challenged to keep their networks safe from threats. The push to incorporate 21st century learning environments, online assessments, and BYOD or 1:1 initiatives as well as legal requirements require network administrators to have visibility into their network's traffic. This can only be accomplished through the use of a next-generation firewall.

The following chapters will discuss firewalls and how the Palo Alto next-generation firewall can be used to secure a K-12 network. Chapter 2 will provide background information on firewalls, including their purpose and types and detail the importance of application layer inspection. It will then discuss Palo Alto Networks and its firewall technologies. Chapter 3 will provide practical uses of the Palo Alto next generation firewalls in securing a K-12 network, which can only be accomplished by using a firewall that inspects traffic at the application layer.

Chapter 4 will provide an example configuration for a hypothetical middle school. A problem scenario will be presented and addressed with a Palo Alto next generation firewall. Finally, Chapter 5 will provide a summary and discuss areas of further research.

2. FIREWALLS

A firewall sits at the edge of a schools network and inspects every incoming and outgoing packet that passes through it. Traditional firewalls work by filtering packets by port and protocol. However, this is not adequate to secure a network today. There is a vast landscape of applications that communicate using standard ports and protocols making traditional access controls obsolete. Traditional firewalls do not have the fine-grained intelligence to distinguish one kind of traffic from another [9]. Blocking only by port and protocol could potentially deny legitimate applications. Firewalls that perform deep packet inspection and classify traffic at the application layer become an extremely valuable tool in securing a network. These are classified as next-generation firewalls or NGFWs.

2.1 Purpose

Firewalls provide security to a network or computer by preventing access to it based on rules or policies [10] [11]. Firewalls are typically located at the perimeter of a network where they act as a "gatekeeper" either allowing or denying packets entering or leaving the network. As data is received by the firewall, the firewall determines whether or not the data can be allowed to pass based on configured rules. Depending on the type of firewall, processing can take place at several different layers as described by the OSI (Open Systems Interconnection) reference model as pictured in Figure 1.

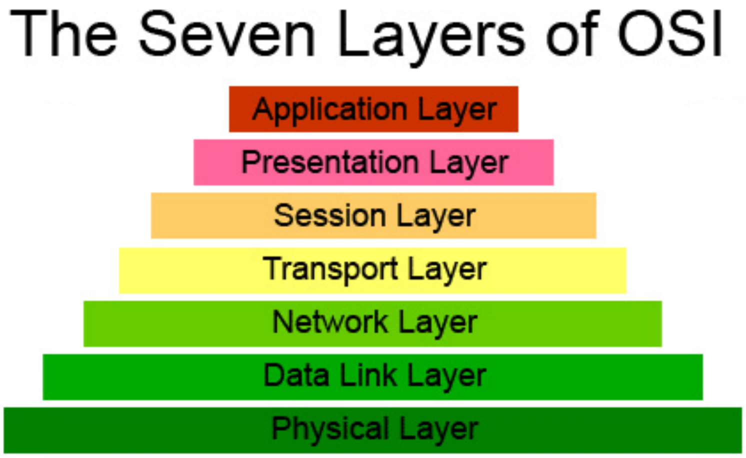


Figure 1. Layers of the OSI Model [12]

2.2 Types of Firewalls

Generally the features of a firewall can help categorize it. Although there is no standard for classification, one way to describe firewalls is by generation: first generation, second generation or next-generation. First generation firewalls are also commonly referred to as stateless firewalls or packet filters and operate at the lower three layers of the OSI model and do not concern themselves with the actual data of a packet. Packet filters look only at source and destination addresses and ports, the protocol in use, the interface or interfaces it traverses and the direction of the packet (inbound or outbound) [13]. Second generation firewalls, also referred to as stateful firewalls, work similarly but use transport layer information to track the state of connections [14]. The additional information can be combined with protocol awareness to allow firewalls to make more intelligent decisions on packets [13]. Next-generation firewalls build upon prior generations by inspecting packets at the Application Layer (Layer 7) of the OSI model [14]. This allows a more detailed look at data traffic and the capability to categorize different types of traffic on the same port [15]. There are also many other important features that have been integrated into firewalls including VPN services, proxy services (both inbound and outbound) and unified threat management [16].

2.3 Importance of Application Layer Firewalls

First and second generations primarily work at Layer 2 and Layer 3 of the OSI model. Although this still has a place in providing network security, it no longer is enough to provide adequate security [16]. With the explosion of applications running on standard ports, it is important the firewall be able to distinguish approved applications from unapproved applications, malware, bots, and viruses. This can only be accomplished with Layer 7 inspection. Layer 7 inspection, also called deep packet inspection, or DPI, is an advanced method of packet filtering which functions at the Application layer of the OSI model [17]. The use of DPI makes it possible to find, identify, classify, reroute or block packets with specific data or code payloads that conventional packet filtering, which examines only packet headers, cannot detect [17]. This is the fundamental basis for many of the advanced technologies NGFWs use.

2.4 Market Leaders

The firewall market has evolved from simple stateful firewalls to NGFWs. Gartner, the world's leading information technology research company, conducts market studies annually about the enterprise firewall market. In its 2013 Magic Quadrant for Enterprise Network Firewalls (pictured below in Figure 2), it describes Check Point Software Technologies, Palo Alto Networks, Fortinet, Cisco and Juniper Networks as the top firewall companies when it comes to vision and execution [18]. Companies such as Check Point, Cisco and Juniper have long been favorites of large corporations and offer NGFWs. Although not as established as the previously mentioned companies, Palo Alto Networks firewall has a great blend of enterprise class features and a simplistic management interface making it a perfect fit for school districts.

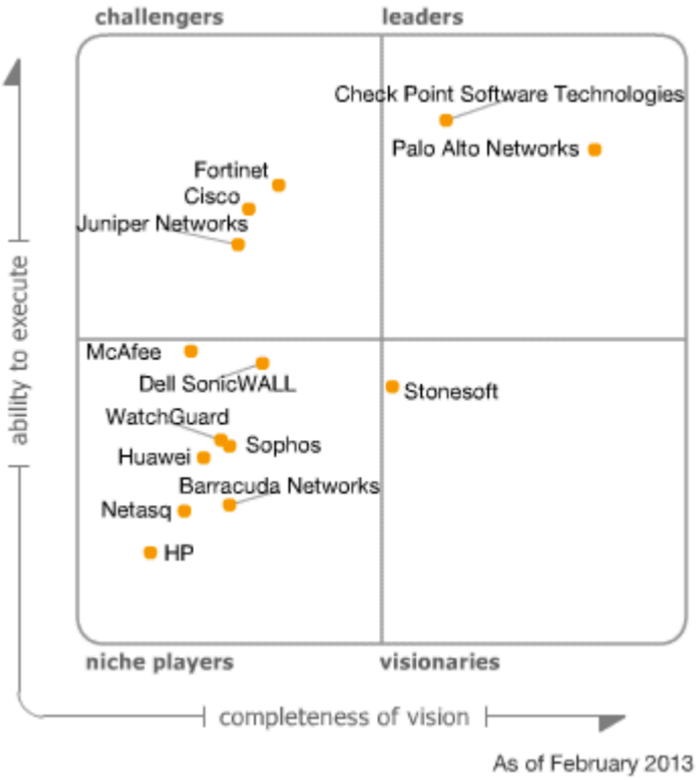


Figure 2. 2013 Gartner Magic Quadrant for Enterprise Network Firewalls [18]

Palo Alto Networks, Inc. is a network security company that has, during its short seven-year existence, become a market leader according to Gartner [18]. Palo Alto produces NGFWs that combine the traditional features of a firewall with advanced traffic classification based on applications and users. These features prove to be extremely useful for K-12 school districts looking to get the most out of their networks [19].

2.5 About Palo Alto Networks, Inc.

Palo Alto Networks, Inc. is a leader in firewall security and has over 19,000 customers in 120 countries [20] [21]. They currently employ over 1,200 employees. Gartner has ranked them amongst the leaders in the enterprise firewall market in 2011, 2012 and 2013 [20]. From the 2013 Gartner Magic Quadrant for Enterprise Network Firewalls, “Palo Alto Networks continues to both drive competitors to react in the firewall market and to move the overall firewall market forward [18]. It is assessed as a Leader, mostly because of its NGFW design, direction of the market along the NGFW path, consistent displacement of competitors, rapidly increasing revenue and market share, and market disruption that forces competitors in all quadrants to react [18].”

2.6 Core Technologies

Palo Alto NGFWs contain three core technologies, which are the foundation of their security platform. These core technologies, App-ID, User-ID and Content-ID, inspect all traffic, on all ports regardless of type. App- ID is a traffic classification system that allows the firewall to identify applications running on the network [22]. Traffic is first classified based on IP and port [22]. The firewall will then use application signatures to classify the traffic. Once traffic is classified, policies will be enforced as needed. User-ID allows more visibility into network traffic by matching traffic to users [23]. Through direct integration into an organization’s directory services, such as Active Directory, data traffic can be classified by application with App-ID and matched to a specific user. It also allows specific policies to be created based on user or group [23]. This is extremely useful for creating application policies that apply to certain groups no matter where they are on the network [23]. Content-ID contains several different features which include IPS, URL filtering and file and data filtering [24].

2.7 Palo Alto in Education

Palo Alto Networks NGFW appliance is an ideal high-performance platform to secure a K-12 school district network. Through the use of three of its core technologies, App-ID, User-ID, and Content-ID, a network administrator can achieve a detailed look into their school's network. With the use of App-ID, network traffic can be classified beyond the traditional port and protocol method. App-ID helps identify applications in use and protects and control users [19]. User-ID allows a network administrator to analyze traffic by user, regardless of where on the network they are connected. By leveraging an existing directory service such as Active Directory, eDirectory or OpenLDAP, traffic can be classified by user by matching user authentication events to device IP addresses. This helps the institution create and enforce dynamic policies to better fulfill security needs. Content-ID represents threat prevention features aimed at controlling unwanted content. These features include IPS, URL filtering and file and data filtering. The IPS feature looks for and blocks known exploits and malware. Reducing malware presence frees up bandwidth [25]. URL filtering controls access to unwanted web sites. This is especially critical for schools to be compliant with CIPA. File and data filtering allows the blocking of specific file types. Through the use of these three core technologies, school network administrators gain the visibility they need to properly secure their network.

2.8 Summary

Firewalls are the "gatekeepers" of the network. They serve a critical function in monitoring traffic and either allowing or denying traffic based on configured rules. As firewalls have evolved over time, differentiating features allow them to be classified into three distinct generations. The most current classification is called "Next-generation". Next-generation firewalls provide application layer inspection giving network administrators detailed information about the applications running on the network. There are many companies that manufacture NGFWs, but Palo Alto has separated itself from the competition.

Palo Alto Networks is a leader in the enterprise firewall market according to Gartner, a leading technology research company. Their next-generation firewalls use three core technologies; App-ID identifies applications, User-ID matches traffic to users and Content-ID prevents threats.   These core technologies give school network administrators the visibility they need to properly secure the network.

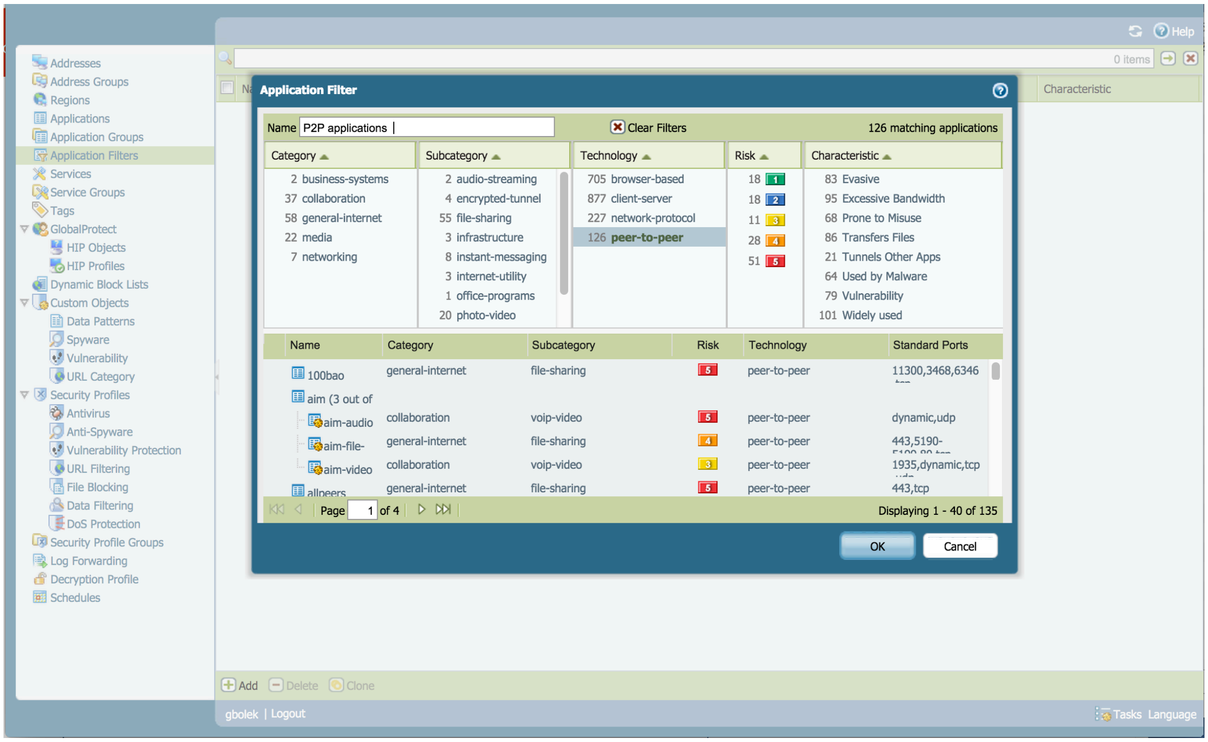
3. USES OF NEXT-GENERATION FIREWALLS IN K-12 SCHOOLS

The are many practical uses for Palo Alto Networks three core technologies, App-ID, User-ID, and Content-ID. This chapter will present scenarios specific to K-12 networks with examples of how each core technology can be applied and why it should be applied. For example, peer-to-peer file sharing applications are a legitimate concern for school administrators and technology staff. Although some serve legitimate purposes, they also are a mechanism for the illegal distribution of copyrighted content and they use valuable network resources. Allowing these applications to run can be a liability for the institution and also a burden to other users on the network. Through the use of App-ID it will be shown how to categorically block peer-to-peer applications. In another example, the use of social media in schools is still debated. Through good policy and user awareness, some schools allow the use of social media applications. Many school districts, however, are still not comfortable with students or even staff accessing social media. Through the use of User-ID it will be detailed how specific policies can be created to allow certain individuals or groups to access social media applications while restricting others. Another scenario will show the use of content filtering. CIPA requires a school district to restrict objectionable content from being viewed by minors. It will be shown, through the use of Content-ID, how URL filtering can be used to block web sites either categorically or individually through custom lists. Through these scenarios and several others, it will be shown how a Palo Alto Networks NGFW can be used to effectively secure a K-12 school network.

3.1 Using App-ID to Block an Application by Category

Although peer-to-peer (P2P) file-sharing application use has been declining, it is still a concern for school network administrators [26]. The concern is not only about bandwidth consumption with P2P applications, but also copyright infringement. Many schools nationwide support BYOD programs so the challenge is how does a school district effectively restrict the use of P2P applications on its network.

Consider a high school student who brings their personal laptop to school and has a P2P application installed. Once the laptop connects to the network it registers itself and begins downloading and uploading files. Even without the intention to use it, many P2P applications run in the background continuously and do not need to be manually started by the user. It is even possible that the user may be completely unaware the application is running. Now with the application running, there is a potential active threat on the network. Using App-ID, the Palo Alto can discover applications of these types running on the network. Also, all applications of this nature can be prevented from functioning by categorically blocking all P2P applications in a security policy. Although this does not keep the application from running on the student's laptop, it does prevent it from creating connections over the network, keeping it from working properly. In order to block all P2P applications, an application filter must be created that is based on the "peer-to-peer" category. This is illustrated in Figure 3. Once the filter is created, it can be used in a security policy that is set to deny matching traffic. Using the application filter will also future-proof the rule. When updates are released by Palo Alto to their "Applications and Threats" database, they will automatically be incorporated into the rule whenever the "peer-to-peer" category is updated.



Name P2P applications

126 matching applications

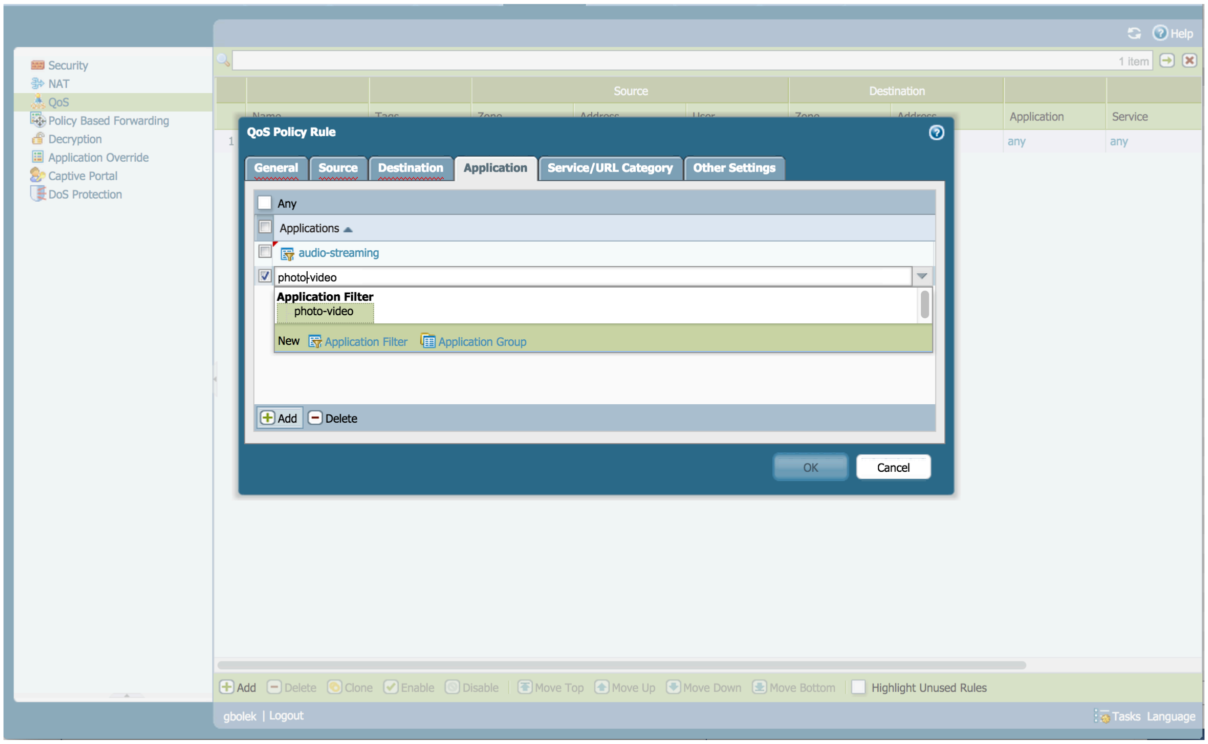
Category	Subcategory	Technology	Risk	Characteristic
2 business-systems	2 audio-streaming	705 browser-based	18 1	83 Evasive
37 collaboration	4 encrypted-tunnel	877 client-server	18 2	95 Excessive Bandwidth
58 general-internet	55 file-sharing	227 network-protocol	11 3	68 Prone to Misuse
22 media	3 infrastructure	126 **peer-to-peer**	28 4	86 Transfers Files
7 networking	8 instant-messaging		51 5	21 Tunnels Other Apps
	3 internet-utility			64 Used by Malware
	1 office-programs			79 Vulnerability
	20 photo-video			101 Widely used

Name	Category	Subcategory	Risk	Technology	Standard Ports
100bao	general-internet	file-sharing	5	peer-to-peer	11300,3468,6346
aim (3 out of					
aim-audio	collaboration	voip-video	5	peer-to-peer	dynamic,udp
aim-file-	general-internet	file-sharing	4	peer-to-peer	443,5190-
aim-video	collaboration	voip-video	3	peer-to-peer	1935,dynamic,tcp
allpeers	general-internet	file-sharing	5	peer-to-peer	443,tcp

Page 1 of 4 Displaying 1 - 40 of 135

Figure 3. Creating the P2P Application Filter

Another group of bandwidth excessive applications is streaming audio and video. According to recent studies, YouTube and Netflix combine for almost half of all Internet traffic [27]. The same usage is seen on school networks where rich media content is extremely valuable in supplementing instruction. School network administrators, however, cannot block access to these resources because they need to be available to students and teachers. The challenge is to ensure bandwidth is available to users when needed and not exhausted by rich media applications. A common scenario found in schools is a classroom full of students using a cart of laptops to access streaming video. Thirty laptops accessing a YouTube video concurrently could potentially saturate a schools connection to the Internet. Using an application filter that includes the “audio-streaming” and “photo-video” categories, a QoS policy can be created that limits the amount of bandwidth available to all the applications in those selected categories. This is shown in Figure 4. The QoS policy will prevent the network from becoming saturated by these applications and ensure there is bandwidth available for other uses.



QoS Policy Rule

□ Any

□ Applications

□ audio-streaming

☑ photo-video

Application Filter
photo-video

Figure 4. Creating a QoS policy

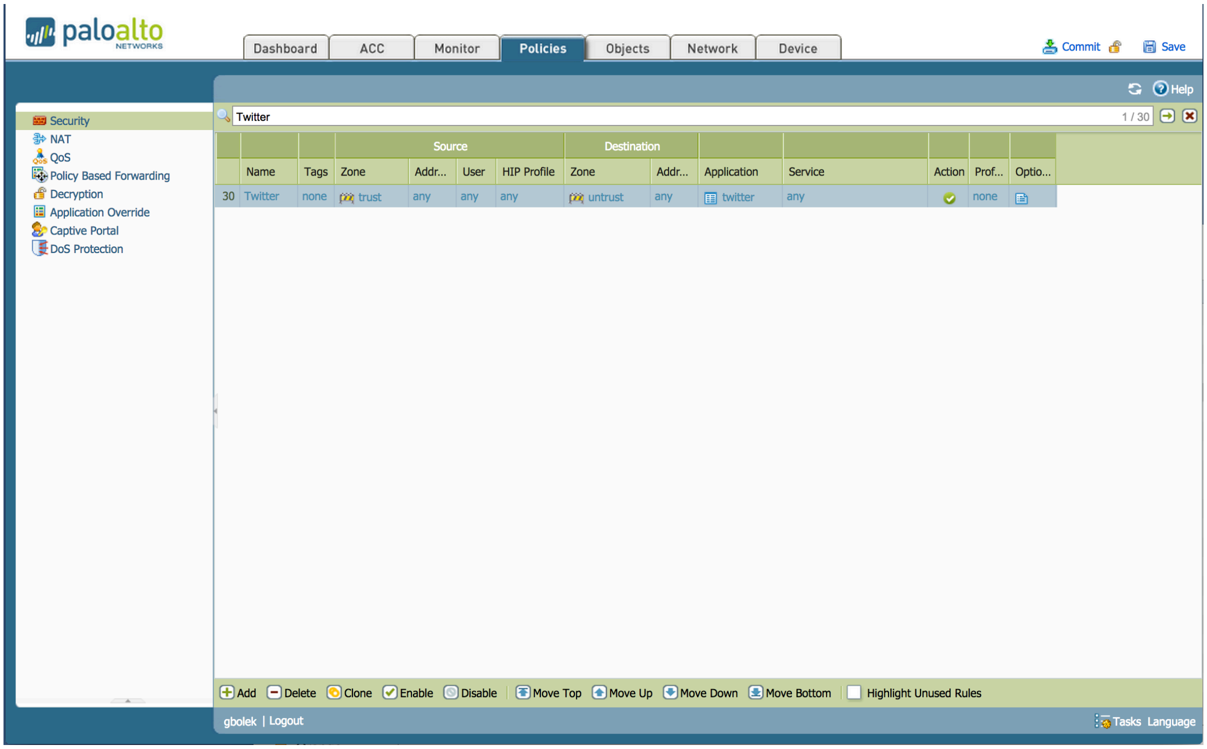
Many school districts are still faced with the challenges of social media. Although some school districts have embraced it, many still do not allow access to social media applications. Prohibiting social media applications is impossible without a NGFW and application layer inspection. With so many different social media applications that are all running on the same standard ports, a firewall must be able to examine Application Layer traffic to successfully stop it from connecting. Using App-ID, a school network administrator can effectively block all social media application from running on the schools network. Many school districts allow network access to students and their mobile devices. This can become problematic if students are accessing Facebook, Snapchat, Twitter and other social media applications from their phones. By creating an application filter based on the “social-networking” category and using the filter in a security policy, the social media applications can be prevented from connecting over the network.

These are three examples of how App-ID application categorization can be effectively used in a school environment. Creating policies based on specific categories of applications allows a network administrator to easily enforce organizational security goals. These examples also illustrate the blocking of application categories, which fits a “permit all” and “block unwanted” security strategy. This may be too lenient, however, for some organizations. In such cases, these same methods can be used in a “block all” and “allow only” strategy. In this strategy, a network administrator permits only certain applications to pass and blocks all other traffic that reaches the firewall.

3.2 Using App-ID to Allow or Block a Specific Application

In the last section, examples were given showing how and why a school district would block entire categories of applications. The last scenario discussed blocking all social media applications with a single “deny” security policy for the “social-networking” category. It is possible, however, a school district may want to allow access to a single application. Imagine the scenario where a teacher would like to have their students’ research on Twitter. The school is already blocking access to all social media applications. This is easily accomplished by creating a new security policy above the previous rule, which permits Twitter traffic only. The Palo Alto firewall (like most firewalls) enforces rules in order from top to bottom. If traffic matches a rule, no further rules are considered. If there is no match, the traffic is matched against the next rule. This continues until the last rule is reached. In this example, a Twitter “allow” rule will be constructed above the rule blocking all social media applications. This is shown in Figure 5.

This gives a school network administrator granular control over which applications are permitted and which are blocked.



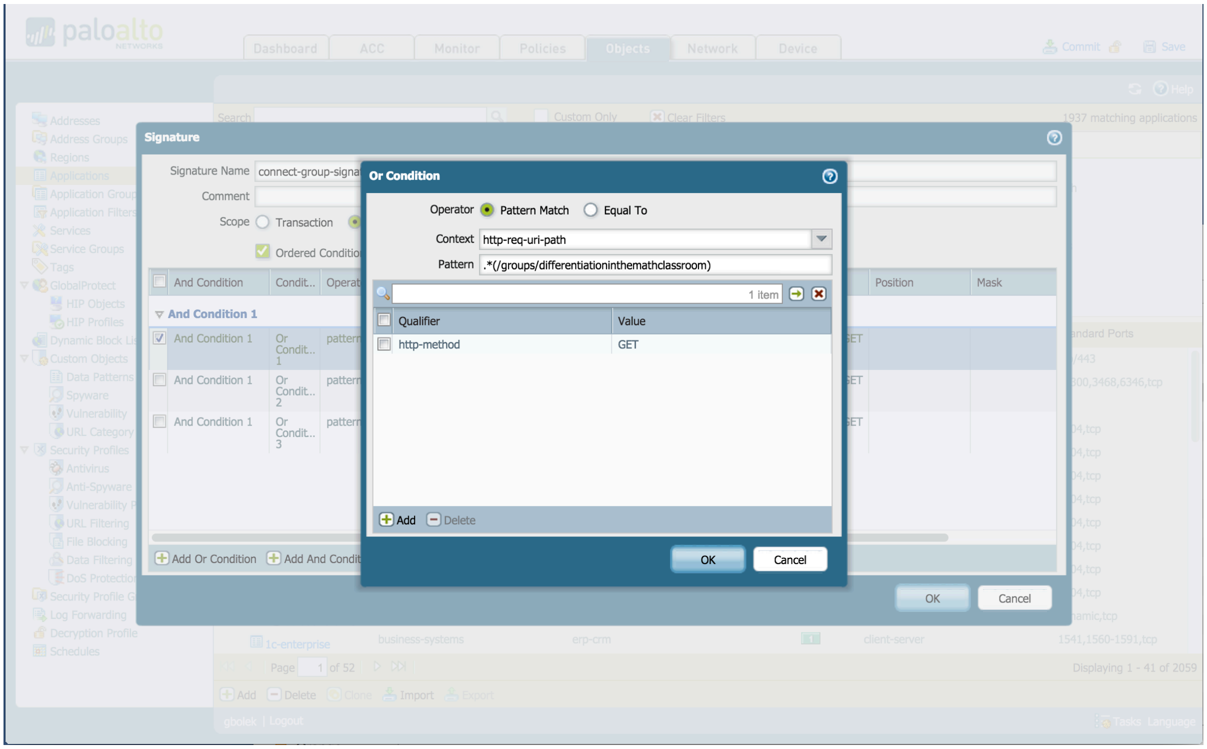
Twitter 1 / 30

			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Service	Action	Prof...	Optio...
30	Twitter	none	trust	any	any	any	untrust	any	twitter	any	✓	none	

Figure 5. Creating the Twitter allow rule

3.3 Using App-ID with Custom Applications

A powerful tool within App-ID is the ability to create custom applications. Palo Alto does provide an extensive library of pre-built application signatures that are updated regularly. There may be circumstances, however, when these signatures are not enough. App-ID allows the creation of custom applications based on the specific criteria needed to block a threat. For example, take a school district that hosts a wiki server that is publicly available. The school district uses the wiki server for both internal and public purposes. Teachers create private wikis for students to access materials, participate in discussions, and submit work. As school policy dictates, these wikis are required to be created with specific permissions so they are not publicly readable or writeable. However, during the creation of a particular wiki, a math teacher forgets to set permissions for the wiki and leaves it publicly readable and writable. Spammers constantly scan for these types opportunities and it is not long before this math wiki is targeted. The wiki server soon becomes overwhelmed with traffic and crashes. After investigation, the school network administrator finds the wiki and 20,000+ new spam entries. The administrator secures the wiki but the spamming continues, crashing the server occasionally. This automated "attack" is continuous and comes from random IP addresses making a single static firewall rule useless. This attack can be mitigated, however, by creating a custom application signature that will look for certain characteristics that are unique to the attack. By performing a packet analysis, the schools network administrator determines that standard HTTP GET and POST commands are overwhelming the server. A custom application is then created that uses a specific URL in the signature. This is illustrated in Figure 6. This custom application is added to a security rule that is set to block all traffic. Using this custom application to block traffic, the school network administrator has successfully mitigated the attack against the wiki server.



Signature Name: connect-group-signa

Comment:

Scope: ○ Transaction

☑ Ordered Conditio

	And Condition	Condit...	Operat
☑	And Condition 1	Or Condit... 1	pattern
□	And Condition 1	Or Condit... 2	pattern
□	And Condition 1	Or Condit... 3	pattern

Or Condition

Operator: ● Pattern Match ○ Equal To

Context: http-req-uri-path

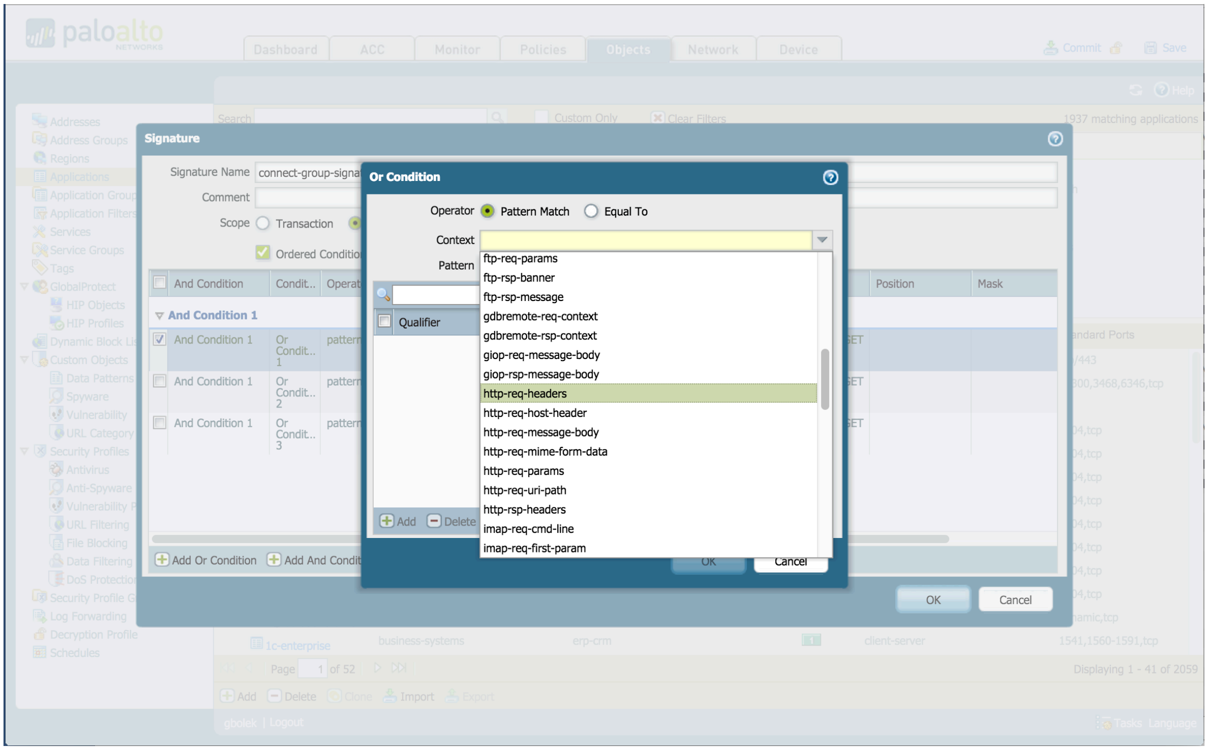
Pattern: .*(/groups/differentiationinthemathclassroom)

1 item

	Qualifier	Value
□	http-method	GET

Figure 6. Constructing the custom application

The capabilities of custom applications are extensive. There are almost 100 different characteristics, or "contexts" as Palo Alto refers to them, which can be searched in a packet. This is shown in Figure 7. DNS, email headers, Java, file, HTTP, SSH, SSL, telnet are all different contexts that can be used. Regular expressions are constructed to search contexts, which provides powerful and flexible searching capabilities. Custom applications can be used to mitigate unique threats, specific to an organization. They can also be used in other policies as well. Custom applications can be created for the proprietary applications of an organization. They can then be used in security policies to enforce specific rules and QoS policies to ensure bandwidth is available. Custom application can also be exported and imported allowing easy sharing between systems or organizations.



Signature

Signature Name connect-group-signa

Scope ○ Transaction

☑ Ordered Conditio

Or Condition

Operator ● Pattern Match ○ Equal To

Context

Pattern

Figure 7. Scrolling through the different custom application contexts

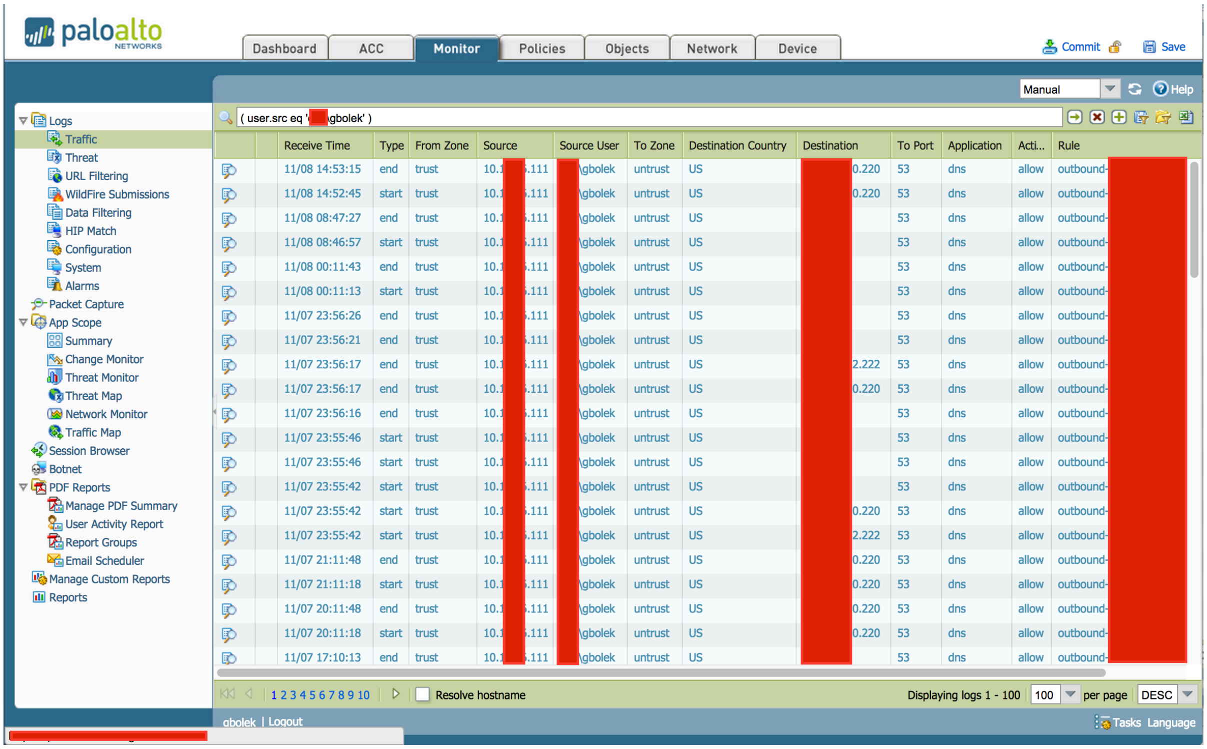
3.4 Using User-ID to Monitor User Activity

User-ID is the second piece of the three core technologies Palo Alto firewalls has created. An important part of managing data traffic in and out of a network is having an understanding of what type of traffic it is and where it originates. App-ID solves this problem by classifying the traffic of hundreds of different types of applications. The other important part of managing data traffic is the understanding of who is creating the traffic. User-ID solves this issue by leveraging an organizations existing directory service and mapping IP addresses to users. By mapping an IP address to a user, all traffic created by the user is identified and reported on within the firewall. This also allows a school network administrator to create meaningful policies that can be dynamic, following a user around the network, regardless of what device the user is using.

At any point during a school day, there can be dozens, hundreds, if not thousands of staff and students on a school district network depending on the size of the school district. Some may be using it for instruction, while others may be leisurely surfing the web during a lunch hour. With so many different users and different activities going on, it is inevitable that at some point a user will cross the line. In circumstances like these, it is important that the school network administrator be able to provide documentation if needed. User-ID assigns traffic to users, allowing the generation of user activity reports. These reports can detail URL categories set to trigger alerts or to be blocked.

3.5 Using User-ID to Create User Specific Policies

Most schools will minimally have four common groups of users: administrators, teachers, staff and students. It is often necessary to grant differing levels of access or have specific security rules dependent on a users classification. User-ID allows the creation of specific security policies based on a single user. For example, consider a school district that has blocked all access to Facebook. If a principal needs access to Facebook, they would have to access it off of the school's network. With User-ID enabled, a school network administrator could create a security policy that enables a single user, the principal, to access Facebook, while still denying all other traffic. This is done quite easily by creating a new security policy and adding the user under the source section of the rule. This policy would be enforced no matter what device the principal was using because User-ID maps the IP address of the device to the user account when the user logs in to a different device. This is an extremely powerful method to grant specific access to users without affecting the network as a whole. These rules can also be enabled or disabled as needed or on demand to further align with an organization's security goals. User-ID can be combined with App-ID to create granular policies, which affect certain users and certain applications. Figure 8 shows the traffic log and user to IP mapping (Private information has been removed). Note the source user column displays the user account associated with the traffic.



(user.src eq '[redacted]\gbolek')

Receive Time	Type	From Zone	Source	Source User	To Zone	Destination Country	Destination	To Port	Application	Acti...	Rule
11/08 14:53:15	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/08 14:52:45	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/08 08:47:27	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/08 08:46:57	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/08 00:11:43	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/08 00:11:13	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:56:26	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:56:21	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:56:17	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]2.222	53	dns	allow	outbound-[redacted]
11/07 23:56:17	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 23:56:16	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:55:46	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:55:46	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:55:42	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]
11/07 23:55:42	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 23:55:42	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]2.222	53	dns	allow	outbound-[redacted]
11/07 21:11:48	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 21:11:18	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 20:11:48	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 20:11:18	start	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]0.220	53	dns	allow	outbound-[redacted]
11/07 17:10:13	end	trust	10.1[redacted].111	[redacted]\gbolek	untrust	US	[redacted]	53	dns	allow	outbound-[redacted]

□ Resolve hostname

Displaying logs 1 - 100   100 per page   DESC

gbolek | Logout

[redacted]

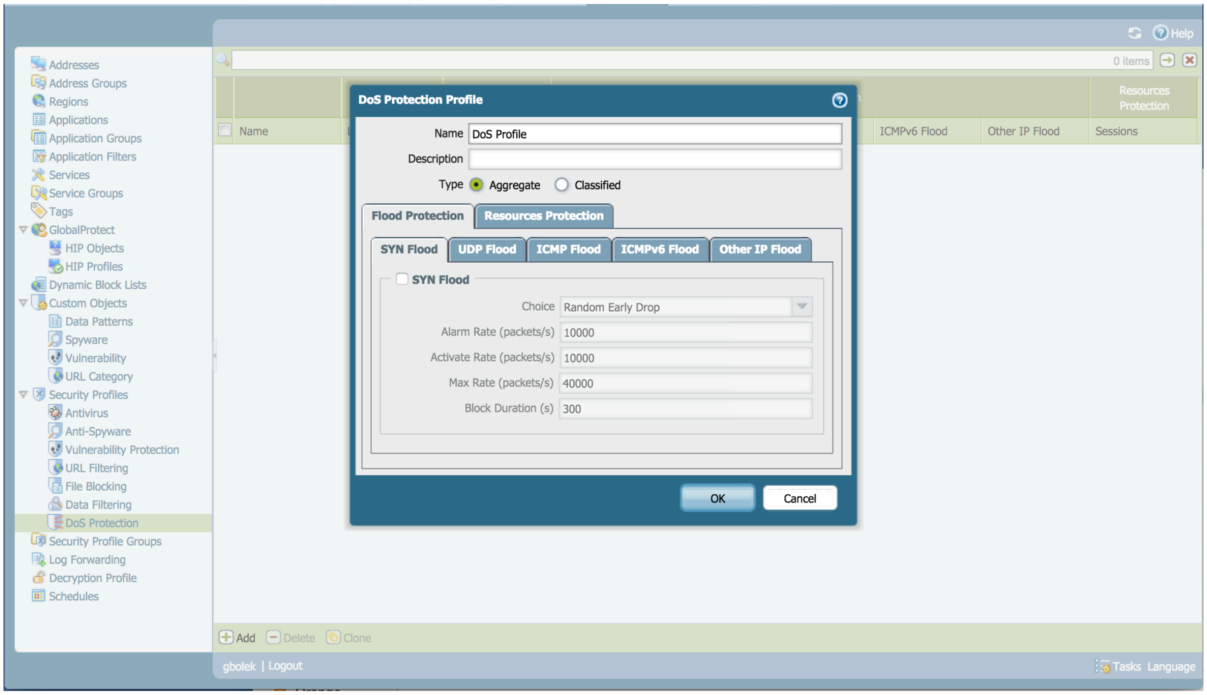
Figure 8. Traffic log showing User to IP mapping

3.6 Using User-ID to Create Group Specific Policies

Another powerful use of User-ID is creating security policies based on user groups. Mentioned earlier, most schools minimally have groups setup for students, staff, teachers and administrators. There are many examples in a school setting where different security policies may be needed for each group. The process to create the rules is similar but instead of entering a user account from the directory, a directory group is used. Limiting social media access is a good example where security policies based on groups can be useful. It is common for administrators to need access to social media sites. This can be achieved using a security rule that explicitly allows the group "administrators" to access the needed application. There is generally a greater need for security policies based on student groups. Grade levels often dictate what resources students can access. Younger students most likely do not need access to social media in comparison to older students. With directory groups created by grade level, it is very easy to create security rules by grade level.

3.7 Using Content-ID to Provide DoS Protection

An important use of Content-ID is the protection of internal resources. School districts hosting internal servers are vulnerable to denial-of-service (DoS) attacks if they are not properly protected. DoS attacks occur when an attacker attempts to overwhelm a computer by bombarding it with traffic. It is common for school district to host servers of varying types such as web servers, wiki servers, email servers, and student information servers. Content-ID allows DoS protection of these resources by creating specific policies. Creating these policies are quickly done. A school network administrator can create a DoS profile and then use the profile in a DoS policy. As illustrated in Figure 9, the profile contains the thresholds for flood protection and resource protection. The flood protection thresholds set limits for SYN, UDP and ICMP flood rates. The resource protection sets limits for sessions. The DoS policy will then enforce this profile. Depending on need, a single profile can be used to protect multiple servers or custom profiles can be created for each internal resource.



DoS Protection Profile

Name: DoS Profile

Description:

Type ● Aggregate ○ Classified

Flood Protection | Resources Protection

SYN Flood | UDP Flood | ICMP Flood | ICMPv6 Flood | Other IP Flood

□ SYN Flood

Choice: Random Early Drop

Alarm Rate (packets/s): 10000

Activate Rate (packets/s): 10000

Max Rate (packets/s): 40000

Block Duration (s): 300

OK | Cancel

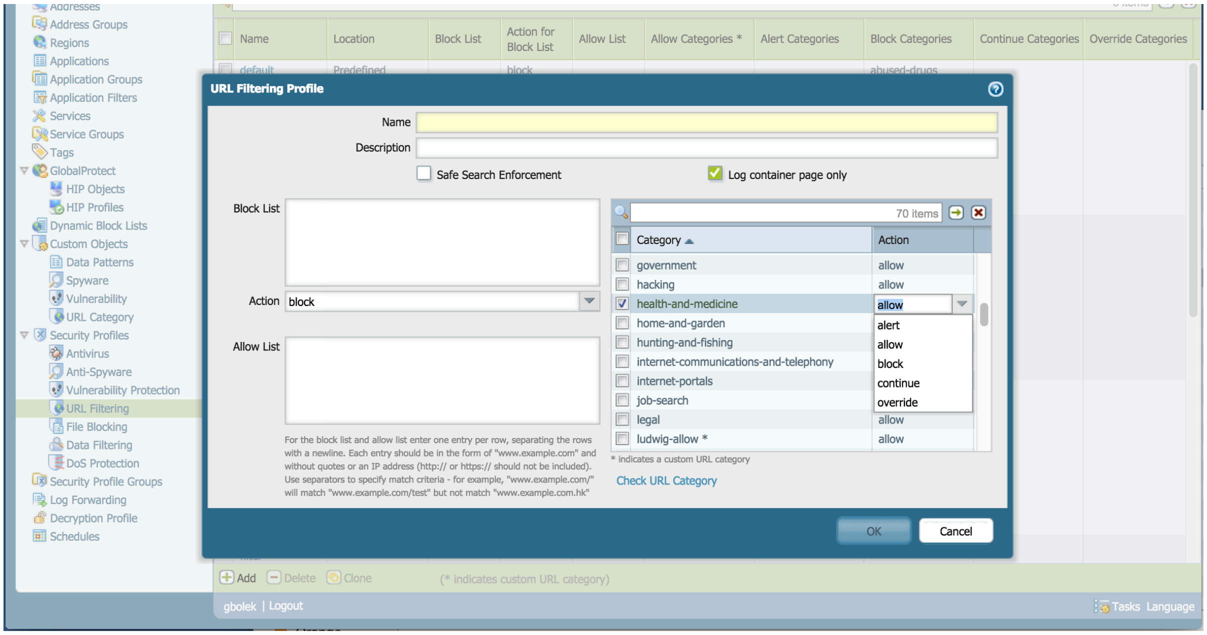
Figure 9. Creating a DoS profile

3.8 Using Content-ID to Provide Anti-Virus and Anti-Spyware Protection

For applications that are allowed to enter the network, it is critical traffic is scanned for viruses and spyware. Palo Alto provides automatic updates to its Anti-Virus definitions to schools can be sure they have current protection. Protecting the network and its resources can be difficult with students having access to the web. Security profiles can be configured with specific scanning parameters. These profiles can then be used in with existing security policies. For example, a school district's firewall will have access rules setup for its network. Minimally, an outbound rule will be needed to allow traffic originating from the internal network to pass to the Internet. A security profile can be added to the rule to use the Anti-Virus and Anti-Spyware scanning. After this is added, all network traffic will be scanned according to the security profile's settings.

3.9 Using Content ID to Provide URL Filtering

Perhaps one of the most critical functions of Content-ID is its URL filtering. As detailed earlier, schools are required by CIPA to block access to content harmful to minors. Content-ID provides URL filtering through Palo Alto Networks proprietary database. Custom URL filtering profiles can then be created based upon the needs of the school. There are over fifty different categories each with its own allow or block settings. This allows great flexibility to how URL filtering is imposed. In addition, there are also custom lists can be created for whitelisting (allowing a specific URL) and blacklisting (blocking a specific URL). When used with User-ID, a school can provide custom filtering for specific users or groups of users. A K-12 school district will have different restrictions based on grade level. High school students will have access to different categories then 1st grade students. For example, the category “Health and Medicine” may be appropriate for high school students and set to allow. This is illustrated in Figure 10. It may be useful for research and class work and the content is also more likely to be age appropriate. In comparison, that category might be inappropriate for 1st grade students. There is the potential for graphic images or other content geared towards older students. In this situation, it may be appropriate to block that category for one group but allow it for another.



URL Filtering Profile

Name

Description

□ Safe Search Enforcement ☑ Log container page only

Block List

Action: block

Allow List

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

70 items

	Category	Action
□	government	allow
□	hacking	allow
☑	health-and-medicine	allow
□	home-and-garden	
□	hunting-and-fishing	
□	internet-communications-and-telephony	
□	internet-portals	
□	job-search	
□	legal	allow
□	ludwig-allow *	allow

alert
allow
block
continue
override

* indicates a custom URL category

Check URL Category

Figure 10. Configuring the Health and Medicine URL category settings

Another useful feature of URL filtering is blacklisting and whitelisting. By creating custom URL categories, a school network administrator can add URLs manually to either be blocked or allowed. Blacklists are custom lists of URLs that are not permitted, while whitelists are URLs that are permitted. URL categorization is not perfect and there are instances when a specific URL is blocked and should not be or vice versa. School network administrators will use both lists in support of their content filtering policies.

3.10 Using Content-ID to Block File Types

Content-ID provides the capability for school network administrators to block unapproved files through the use a of File Blocking profile. Certain file types such as .scr, .exe and .zip are more likely to carry malware. These can be blocked outright or in conjunction with App-ID by application. Students do not often understand the consequences of their browsing. By clicking on links, potentially dangerous files could be saved and executed from the local system causing security issues. Palo Alto contains a list of 100+ file types, which can be added to a File Blocking profile. There is also the capability to create custom data patterns to search for specific patterns of data, such as credit card numbers. For schools needing to protect sensitive information, this can prevent data breaches.

3.11 Summary

There are many practical uses App-ID, User-ID and Content-ID. App-ID can be used to categorically block certain application in schools such as P2P, streaming audio or video and social media applications. It also can be used to allow or deny specific applications to override an existing security policy. A school network administrator can create a custom application to meet specific needs, when the pre-built application signatures are not enough. User-ID matches traffic to a user by leveraging a school's existing directory service. User specific activity reports and security policies can be created. User-ID can also use directory groups in security rules allowing additional flexibility in rule design. Content-ID provides content filtering and threat protection. Maintaining CIPA compliance is important for schools and is easily done using the URL filtering. Content-ID also provides protection from viruses and malware and from DoS attacks.

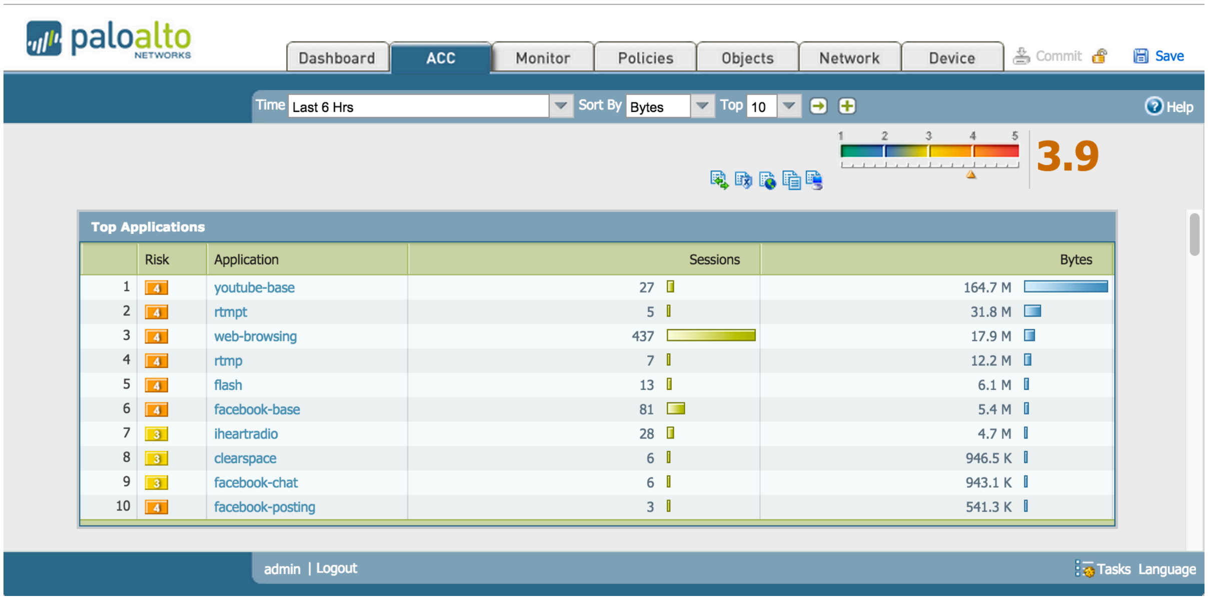
4. CONFIGURING A PALO ALTO FIREWALL FOR A MIDDLE SCHOOL

Grove Middle School (GMS) is a medium-sized school housing three grade levels from 6th to 8th grade. In total, there are 600 students and 60 staff members in the school. The staff members include building administrators, teachers, and support staff. In regards to technology access, GMS has 9 mobile carts each with 30 laptops available for checkout from the library. Teachers check the carts out and use them in their classrooms where students wirelessly access the network.

The school's network infrastructure consists of a single Layer 3 switch to perform simple routing and several Layer 2 switches providing access throughout the school. Wireless access points are located in each classroom providing a high performance wireless network for the schools equipment. The school uses a firewall to connect to their ISP and to control access to and from the network. The school also authenticates all of its users using an Active Directory server.

The past school year saw many frustrations begin to develop, as access to the Internet was often slow and unusable at GMS. Subsequently, the school district's IT administrator was challenged to fix the problem. In reviewing monitoring logs, it was confirmed the local network was performing adequately. The school's network switches were performing up to expectations and no bottlenecks were evident. However, after reviewing data regarding the school's firewall, it was confirmed that the schools Internet connection was reaching its maximum capacity. Unfortunately, the IT administrator could not provide any additional information about what was consuming all the bandwidth. GMS was using an older second-generation firewall, which lacked the capability to inspect traffic in the Application Layer. After presenting the findings to the administration, a recommendation to purchase and deploy a Palo Alto next-generation firewall was accepted. A Palo Alto NGFW was purchased and deployed before the end of the school year.

With the Palo Alto in place, the firewall classified traffic immediately using App-ID. After analyzing the network traffic, the school IT administrator easily identified the applications consuming the most bandwidth. As seen in Figure 11, streaming audio and video applications, such as YouTube, flash, and iHeartradio were the top applications in terms of bytes downloaded. These applications were the cause of the network slow downs at GMS and needed to be controlled. Along with these findings, the school IT administrator also was able to identify Facebook use. GMS instituted a policy against the use of social media by students during school hours. The school IT administrator needed to prevent access to these applications as well.



Time Last 6 Hrs Sort By Bytes Top 10

Top Applications

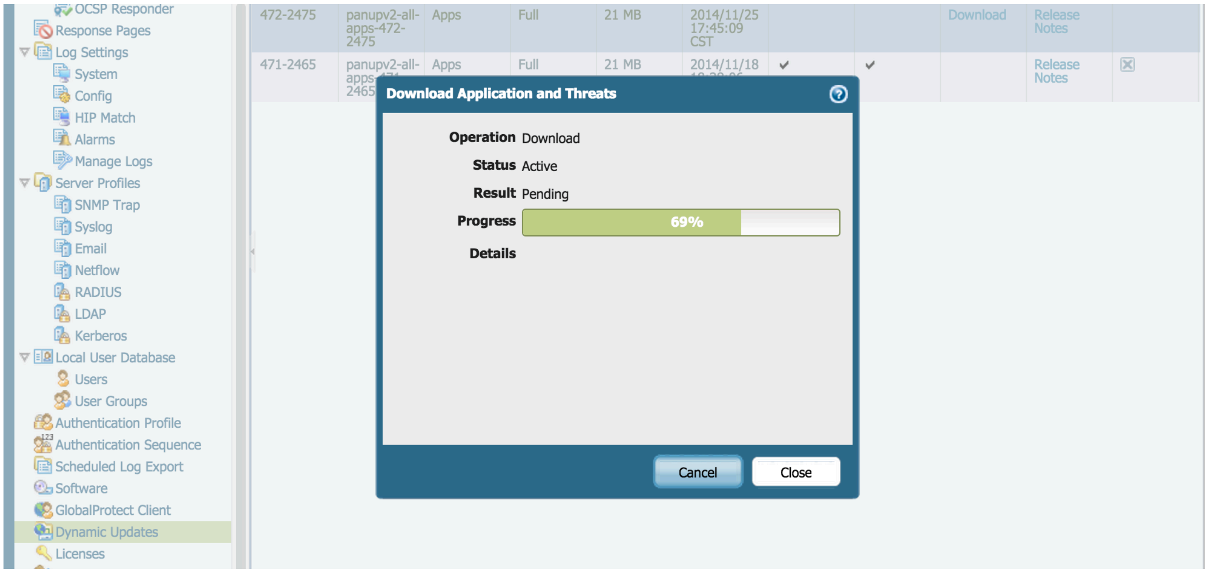
	Risk	Application	Sessions	Bytes
1	4	youtube-base	27	164.7 M
2	4	rtmpt	5	31.8 M
3	4	web-browsing	437	17.9 M
4	4	rtmp	7	12.2 M
5	4	flash	13	6.1 M
6	4	facebook-base	81	5.4 M
7	3	iheartradio	28	4.7 M
8	3	clearspace	6	946.5 K
9	3	facebook-chat	6	943.1 K
10	4	facebook-posting	3	541.3 K

Figure 11. Observing top applications in bytes

The school IT administrator met with GMS administrators and developed a policy for blocking streaming content and social media. It mandated the following: streaming audio should be blocked for all users, streaming video should be blocked for all users except staff, social media access should be blocked for all users, and Twitter access should be allowed for the principal of GMS, Bob Jones, only. Now that the school IT administrator had the new school policy, the next step was to configure the Palo Alto firewall.

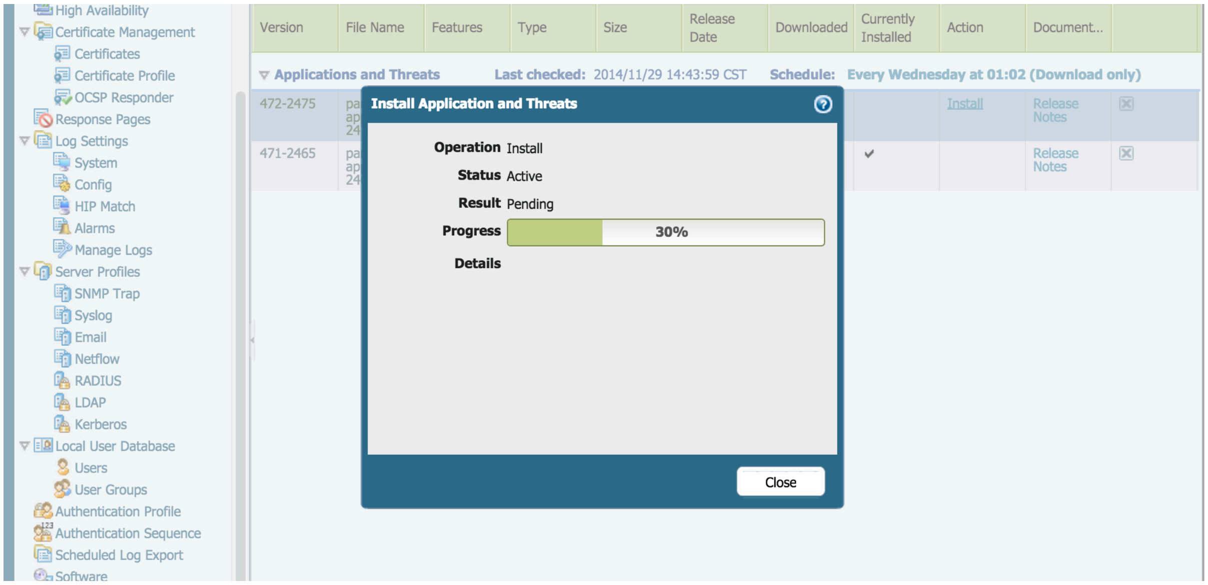
4.1 Configuring App-ID and Content-ID

Looking closer at the new school policy, the school IT administrator determined App-ID, User-ID and Content-ID would all have to be used to be successful. Several new security rules needed to be created but some additional configuration was needed first. App-ID did not require any additional setup before being used, but the newest App signatures were downloaded (Figure 12), installed (Figure 13) and verified (Figure 14).



Operation Download
Status Active
Result Pending
Progress 69%
Details

Figure 12. Downloading the newest Application signatures



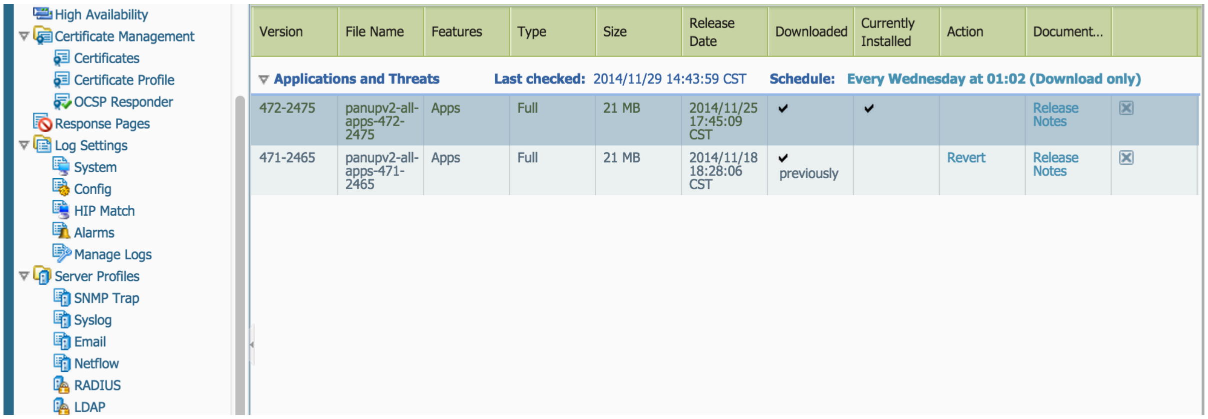
Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Document...
Applications and Threats	Last checked: 2014/11/29 14:43:59 CST	Schedule: Every Wednesday at 01:02 (Download only)							
472-2475	pa ap 24							Install	Release Notes ☒
471-2465	pa ap 24						✓		Release Notes ☒

Install Application and Threats

Operation Install
Status Active
Result Pending
Progress 30%
Details

Close

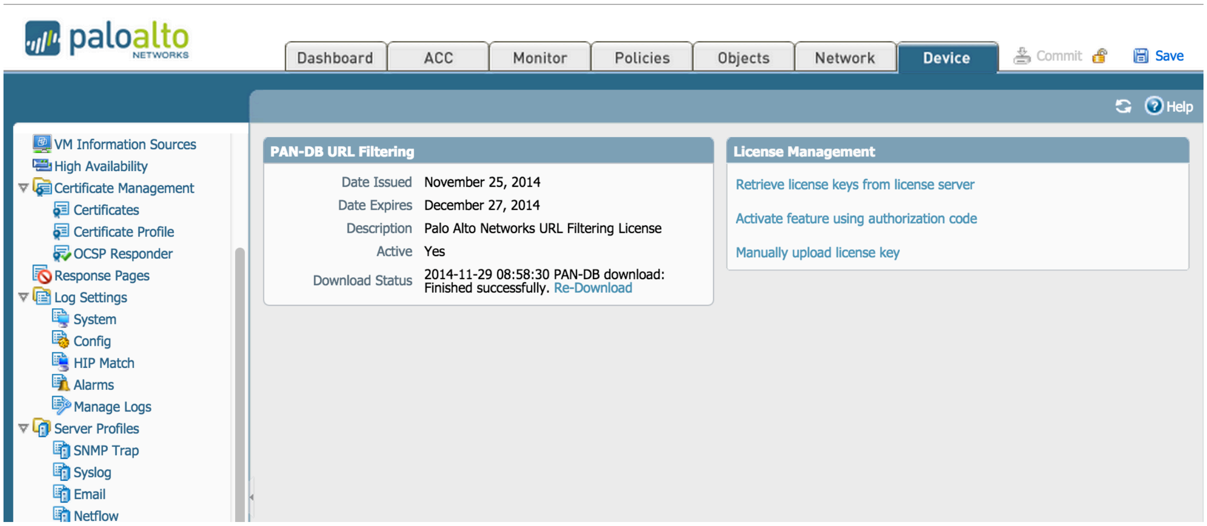
Figure 13. Installing Application signatures updates



Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Document...
Applications and Threats	Last checked: 2014/11/29 14:43:59 CST	Schedule: Every Wednesday at 01:02 (Download only)							
472-2475	panupv2-all-apps-472-2475	Apps	Full	21 MB	2014/11/25 17:45:09 CST	✓	✓		Release Notes ☒
471-2465	panupv2-all-apps-471-2465	Apps	Full	21 MB	2014/11/18 18:28:06 CST	✓ previously		Revert	Release Notes ☒

Figure 14. Verifying updates installed

Content-ID did not require additional configuration, but the download status of the database was confirmed (Figure 15).



PAN-DB URL Filtering

Date Issued	November 25, 2014
Date Expires	December 27, 2014
Description	Palo Alto Networks URL Filtering License
Active	Yes
Download Status	2014-11-29 08:58:30 PAN-DB download: Finished successfully. Re-Download

License Management

Retrieve license keys from license server

Activate feature using authorization code

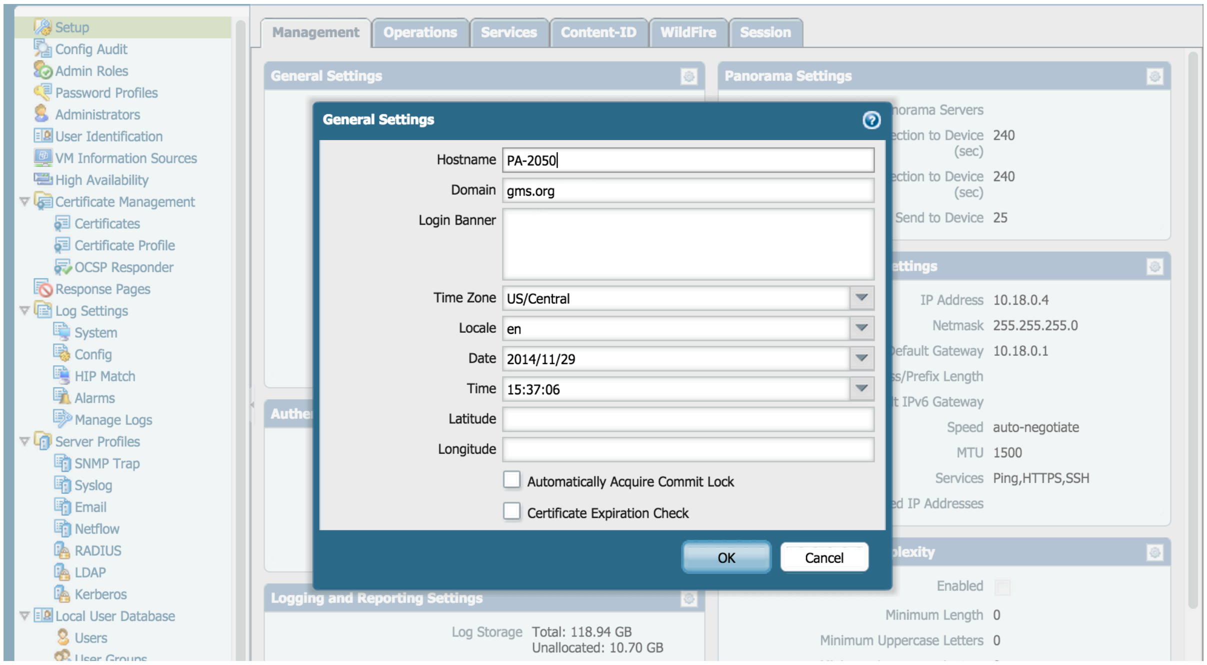
Manually upload license key

Figure 15. Confirming URL database status

User-ID, however, required several additional configuration steps be completed in order to use the existing Active Directory users and groups in security policies. The school IT administrator performed the following steps to get the Palo Alto ready for User-ID.

4.2 Configuring User-ID

The Active Directory domain for GMS was configured as “gms.org” and needed to be set in the Device > Setup > Management > General Settings section as seen in Figure 16. If this is not set correctly, the Palo Alto cannot discover local directory servers and User to IP mappings can fail.



General Settings

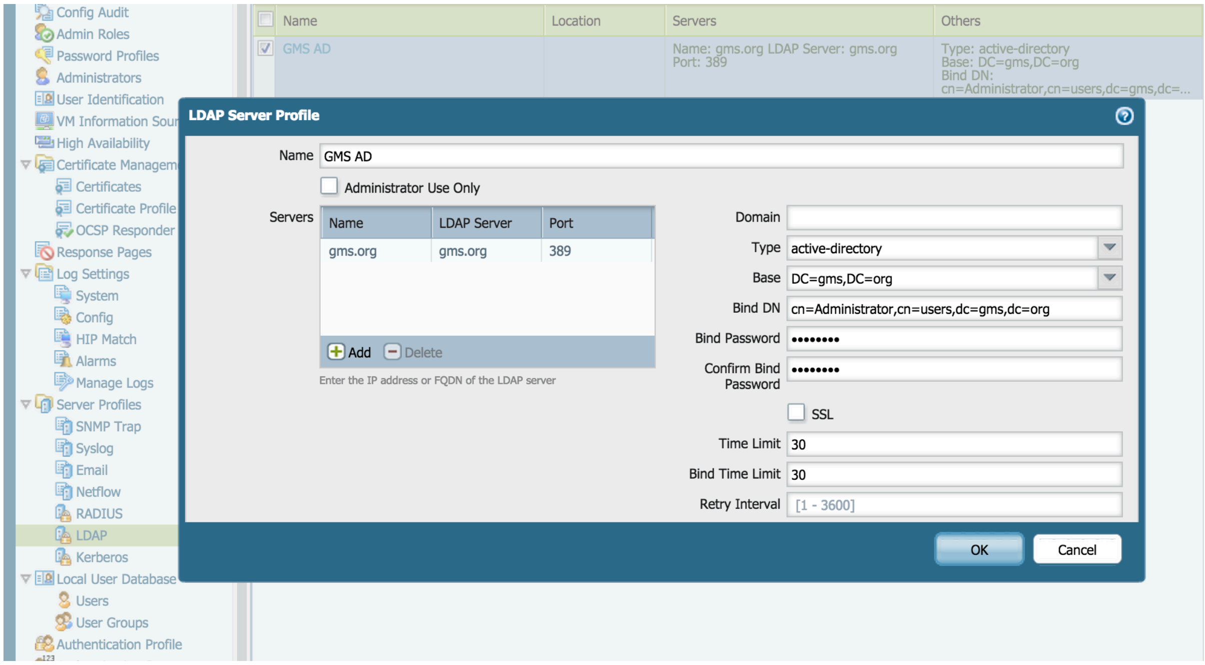
Hostname	PA-2050
Domain	gms.org
Login Banner	
Time Zone	US/Central
Locale	en
Date	2014/11/29
Time	15:37:06
Latitude	
Longitude	

□ Automatically Acquire Commit Lock

□ Certificate Expiration Check

Figure 16. Setting the Active Directory domain

In Device > Server Profiles > LDAP, an entry was created for the GMS Active Directory server (Figure 17). This would be needed later in the Group Mapping settings.



Name	Location	Servers	Others
GMS AD		Name: gms.org LDAP Server: gms.org Port: 389	Type: active-directory Base: DC=gms,DC=org Bind DN: cn=Administrator,cn=users,dc=gms,dc=...

LDAP Server Profile

Name: GMS AD

□ Administrator Use Only

Servers

Name	LDAP Server	Port
gms.org	gms.org	389

Enter the IP address or FQDN of the LDAP server

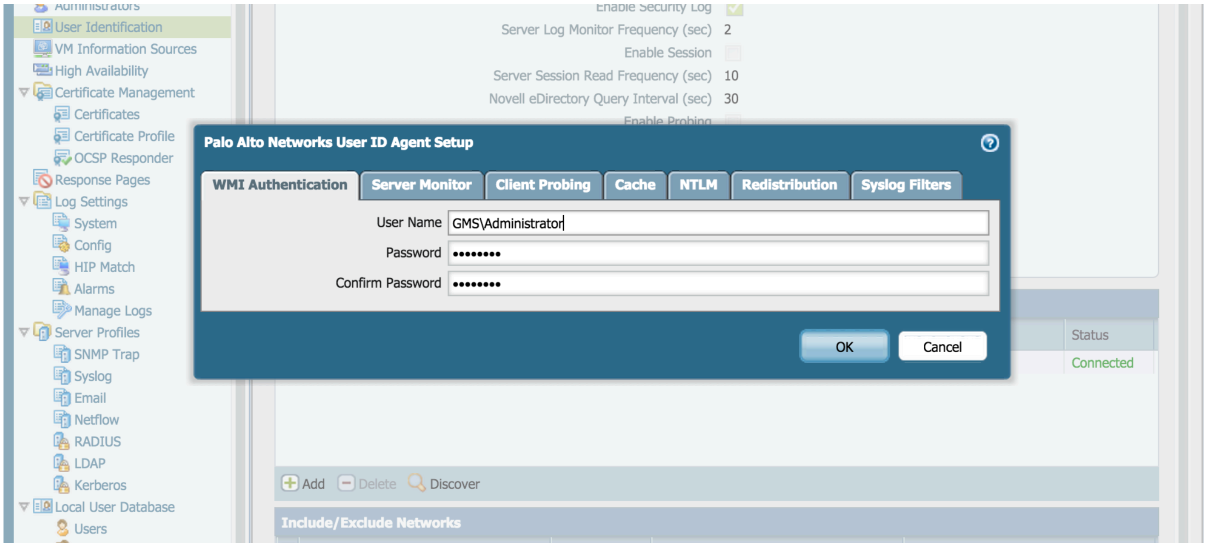
Domain	
Type	active-directory
Base	DC=gms,DC=org
Bind DN	cn=Administrator,cn=users,dc=gms,dc=org
Bind Password	••••••••
Confirm Bind Password	••••••••

□ SSL

Time Limit	30
Bind Time Limit	30
Retry Interval	[1 - 3600]

Figure 17. Creating the server profile for the Active Directory server

Next, the User Mapping and Group Mapping Settings were configured under Device > User Identification. Under User Mapping > Palo Alto Networks User ID Agent Setup the username and password for WMI Authentication were also set (Figure 18).



Enable Security Log ☑
Server Log Monitor Frequency (sec) 2
Enable Session □
Server Session Read Frequency (sec) 10
Novell eDirectory Query Interval (sec) 30
Enable Probing □

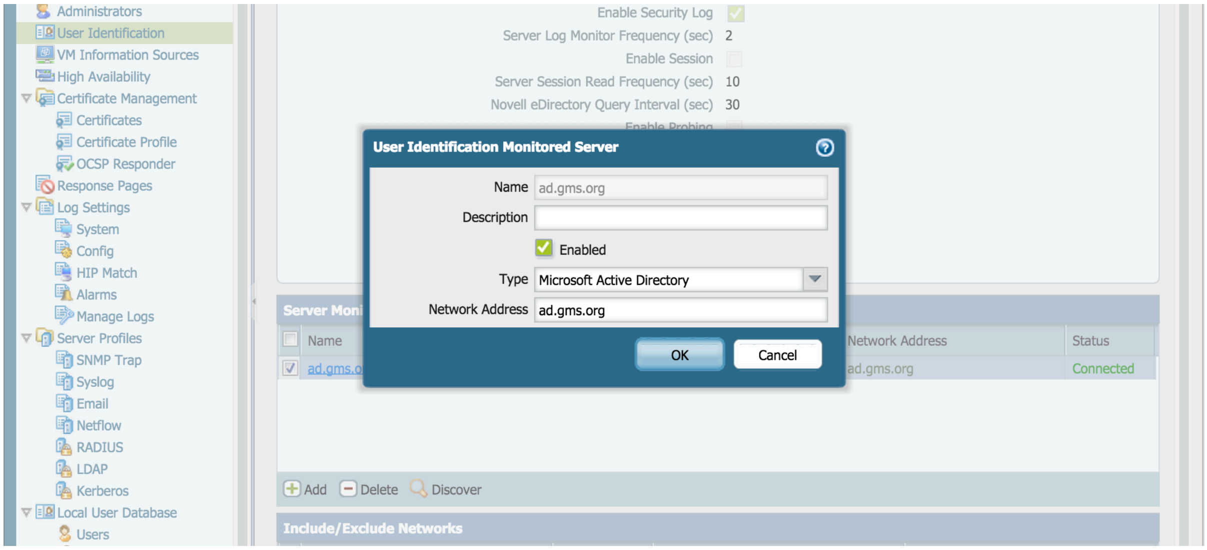
Palo Alto Networks User ID Agent Setup

User Name GMS\Administrator
Password ••••••••
Confirm Password ••••••••

Status: Connected

Figure 18. Palo Alto User-ID Agent setup

In the Server Monitoring section, the "Discover" button was clicked to automatically add the school's Active Directory server (Figure 19)



Enable Security Log ☑
Server Log Monitor Frequency (sec) 2
Enable Session □
Server Session Read Frequency (sec) 10
Novell eDirectory Query Interval (sec) 30
Enable Probing □

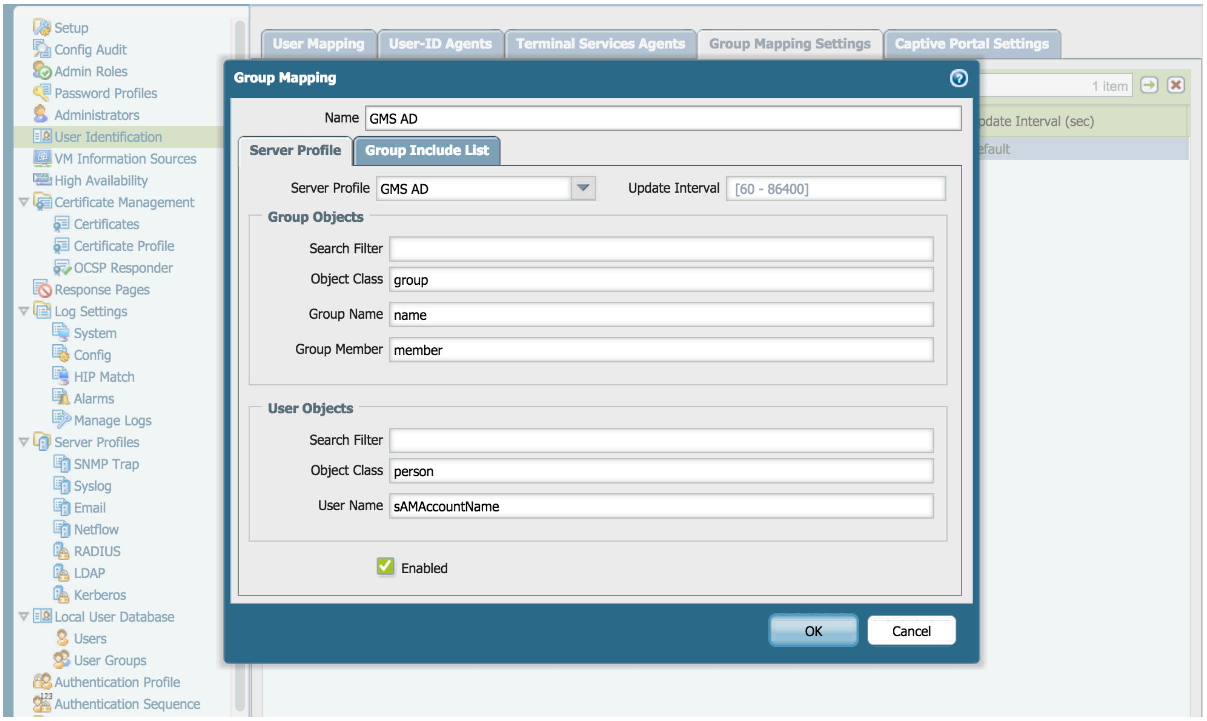
User Identification Monitored Server

Name ad.gms.org
Description
☑ Enabled
Type Microsoft Active Directory
Network Address ad.gms.org

Name	Network Address	Status
☑ ad.gms.o	ad.gms.org	Connected

Figure 19. Discovering the Active Directory server

In the Group Mapping Settings, the LDAP server profile was selected and the default settings were used (Figure 20). By navigating to the Group Include List, the connection was confirmed by verifying the groups in the "Available Groups" section as seen in Figure 21.



Group Mapping

Name GMS AD

Server Profile GMS AD

Update Interval [60 - 86400]

Group Objects

Search Filter

Object Class group

Group Name name

Group Member member

User Objects

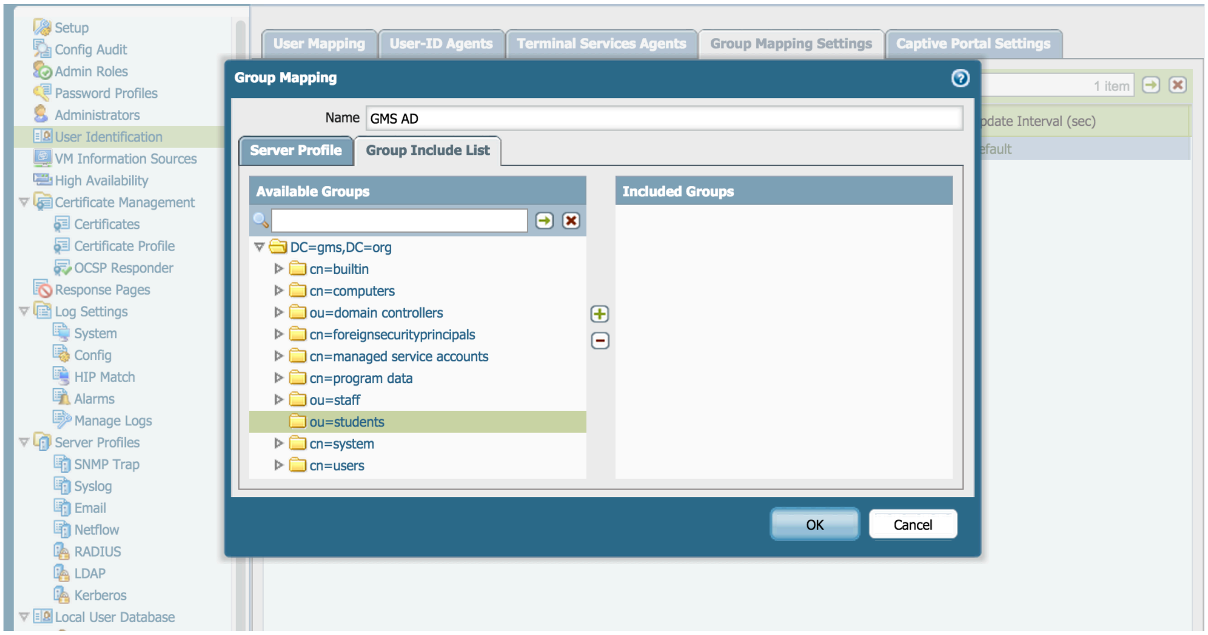
Search Filter

Object Class person

User Name sAMAccountName

☑ Enabled

Figure 20. Configuring Group Mapping Settings



Group Mapping

Name GMS AD

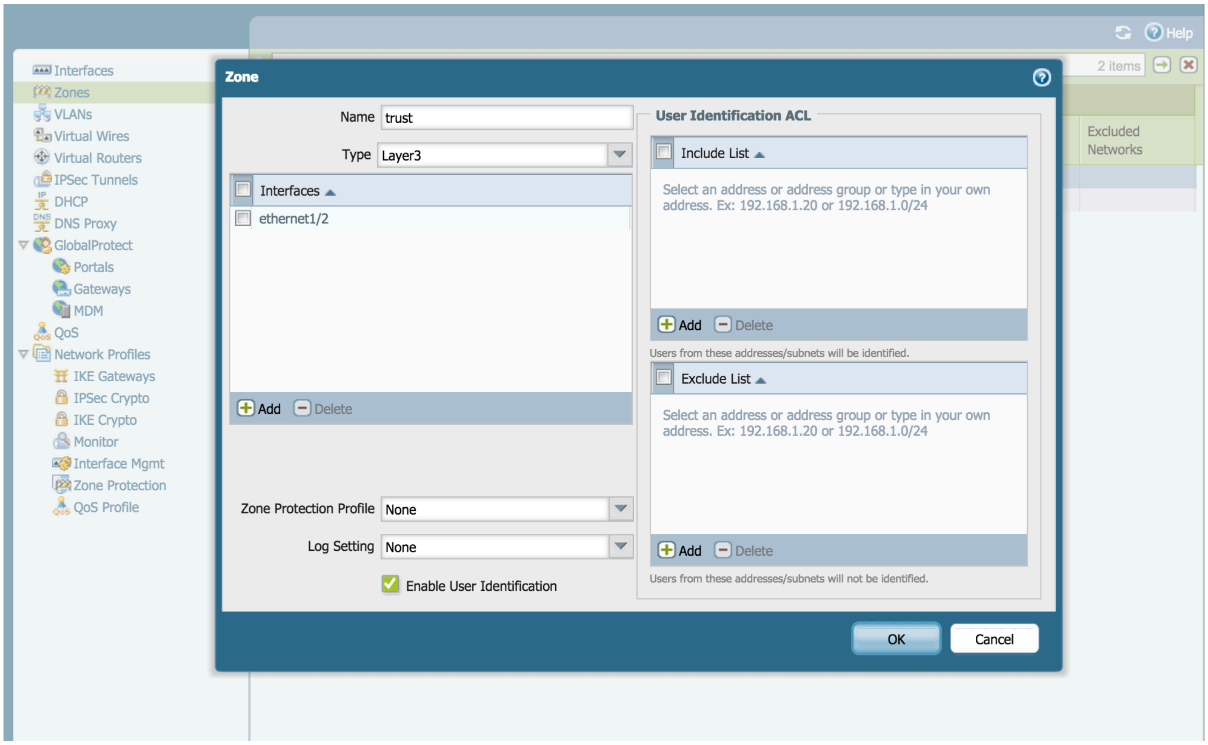
Available Groups

- DC=gms,DC=org
  - cn=builtin
  - cn=computers
  - ou=domain controllers
  - cn=foreignsecurityprincipals
  - cn=managed service accounts
  - cn=program data
  - ou=staff
  - ou=students
  - cn=system
  - cn=users

Included Groups

Figure 21. Browsing the available groups

The final step in configuring User-ID was to enable User-ID for the network security zones configured on the firewall. Security zones are used by the firewall to process traffic. GMS uses 2 zones, “trust” and “untrust”. Internal traffic was assigned to the “trust” zone and external traffic was assigned to the “untrust” zone. User-ID must be enabled on a security zone for it to function. User-ID was enabled for the “trust” zone (Figure 22).



Zone

Name: trust

Type: Layer3

Interfaces: ethernet1/2

Zone Protection Profile: None

Log Setting: None

☑ Enable User Identification

User Identification ACL

Include List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

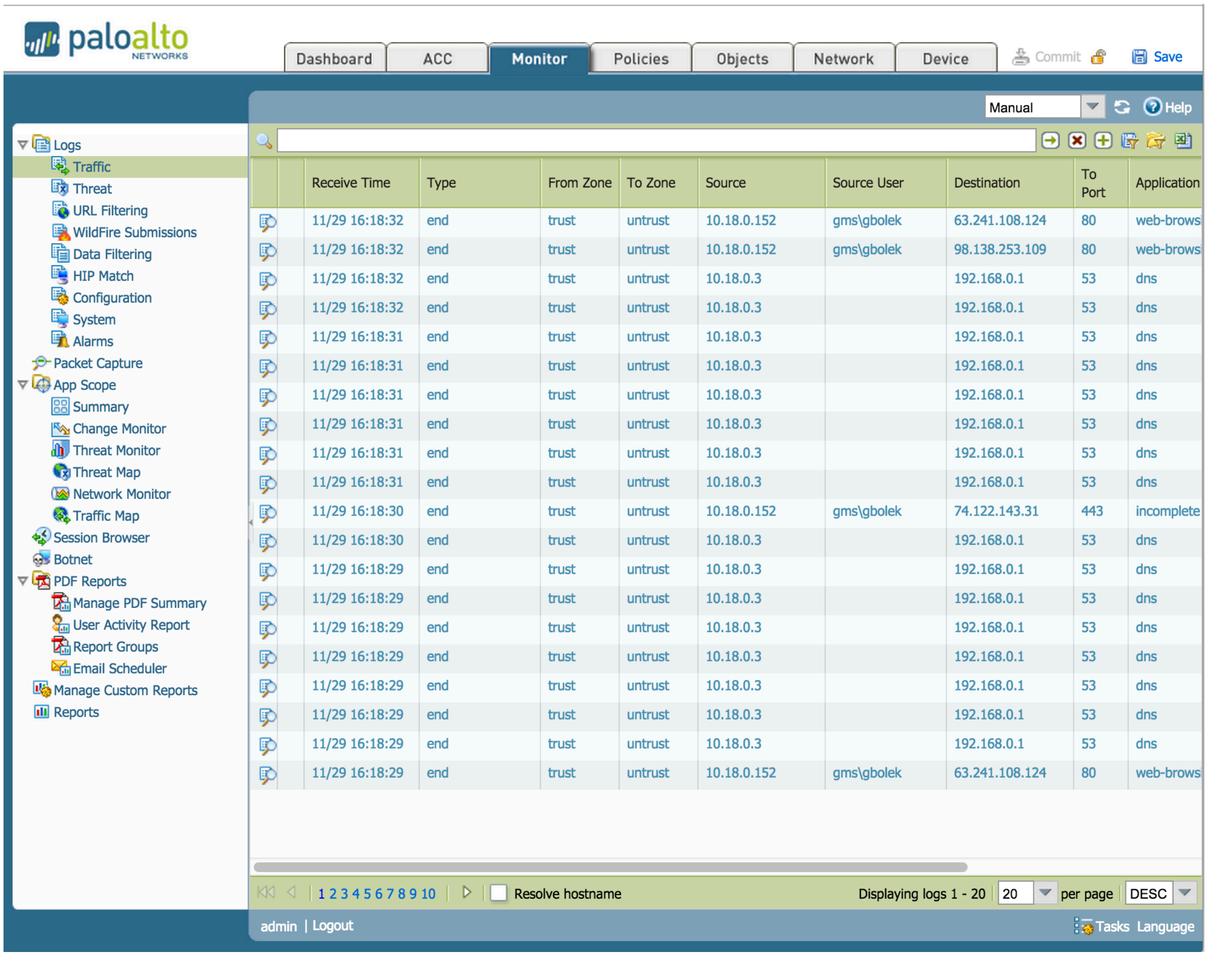
Users from these addresses/subnets will be identified.

Exclude List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Figure 22. Enabling User-ID for the a security zone

After completing the User-ID configuration, User to IP mappings were confirmed by seeing source users in the traffic log (Figure 23).



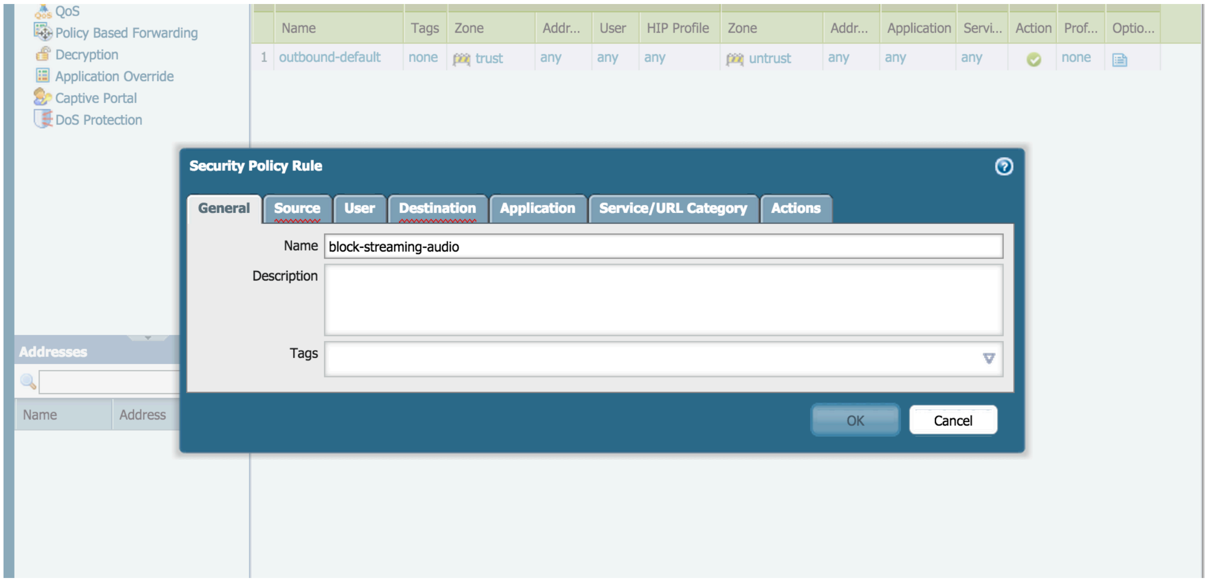
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
11/29 16:18:32	end	trust	untrust	10.18.0.152	gms\gbolek	63.241.108.124	80	web-brows
11/29 16:18:32	end	trust	untrust	10.18.0.152	gms\gbolek	98.138.253.109	80	web-brows
11/29 16:18:32	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:32	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:31	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:30	end	trust	untrust	10.18.0.152	gms\gbolek	74.122.143.31	443	incomplete
11/29 16:18:30	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns
11/29 16:18:29	end	trust	untrust	10.18.0.152	gms\gbolek	63.241.108.124	80	web-brows

Figure 23. Checking the traffic logs for source user mappings

Now that the User-ID setup was completed, the next step was to create security rules.

4.3 Creating the Streaming Audio Rule

Under Policies > Security, the first security rule needed was to block streaming audio for all users. The rule was created by clicking add and then entering information into each tab. The rule was named “block-streaming-audio” in Figure 24.



	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

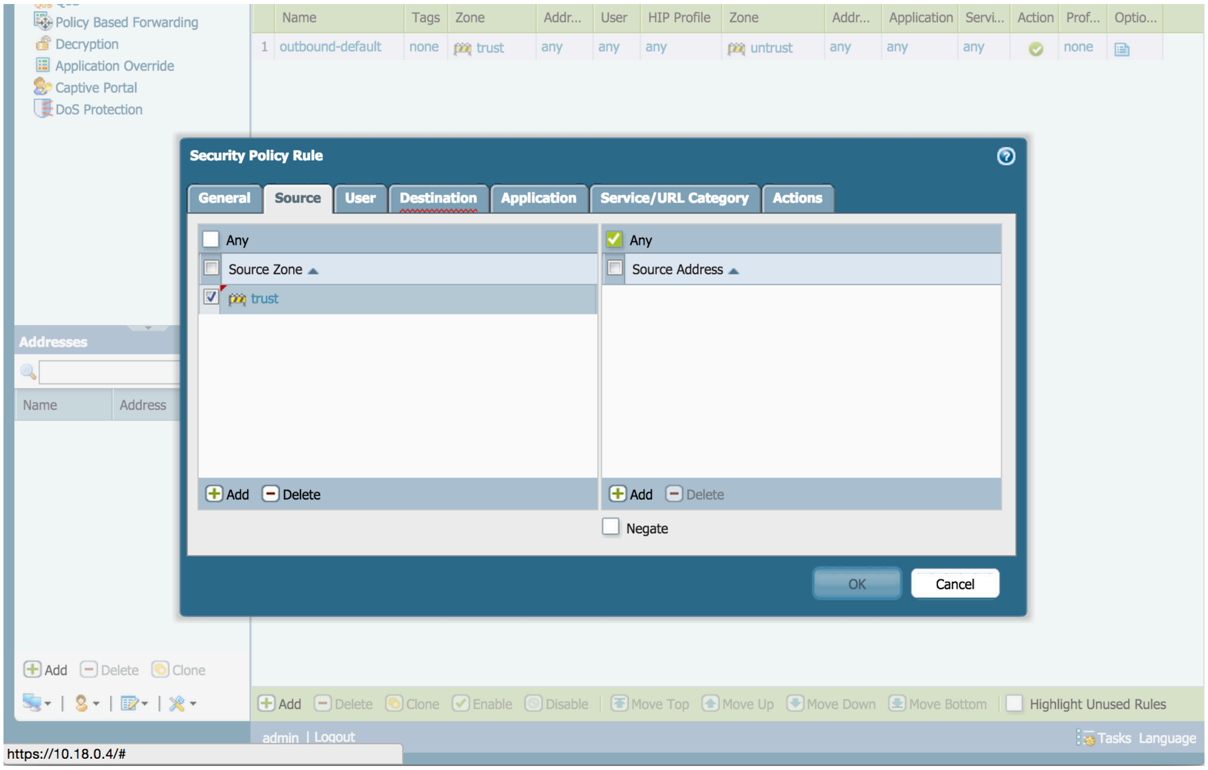
Name: block-streaming-audio

Description:

Tags:

Figure 24. Naming the security rule "block-streaming-audio"

In the User (Figure 25) and Destination (Figure 26) tab, the security zones are set appropriately.



	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

☐ Any

☐ Source Zone

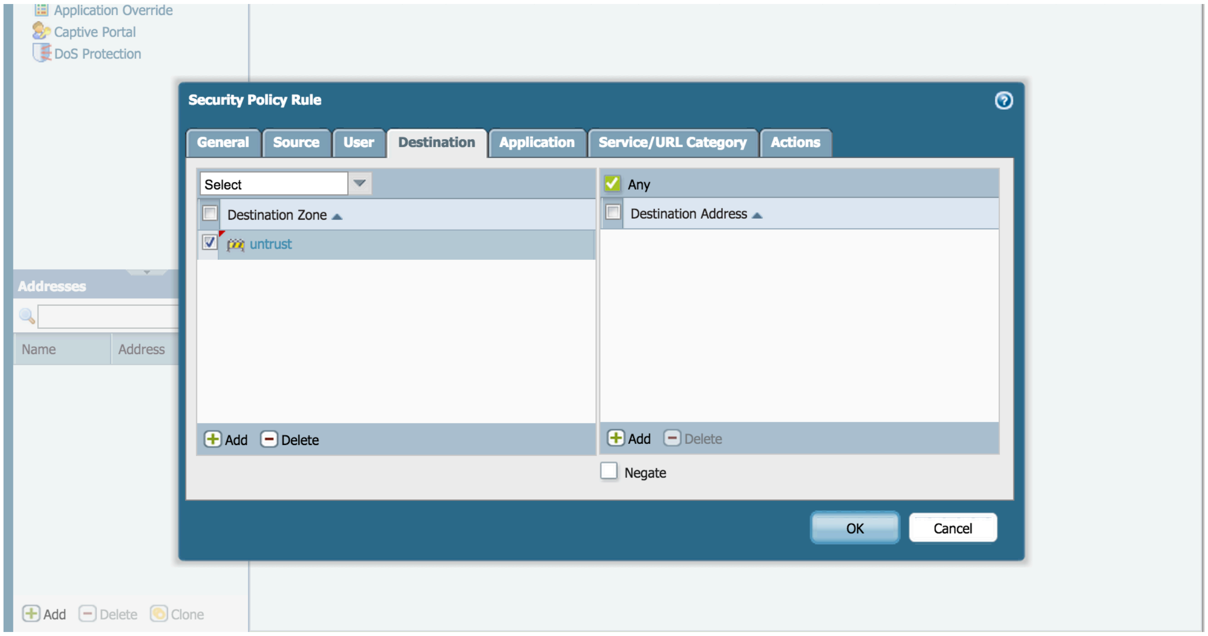
☑ trust

☑ Any

☐ Source Address

☐ Negate

Figure 25. Setting the source security zone



Select

☐ Destination Zone

☑ untrust

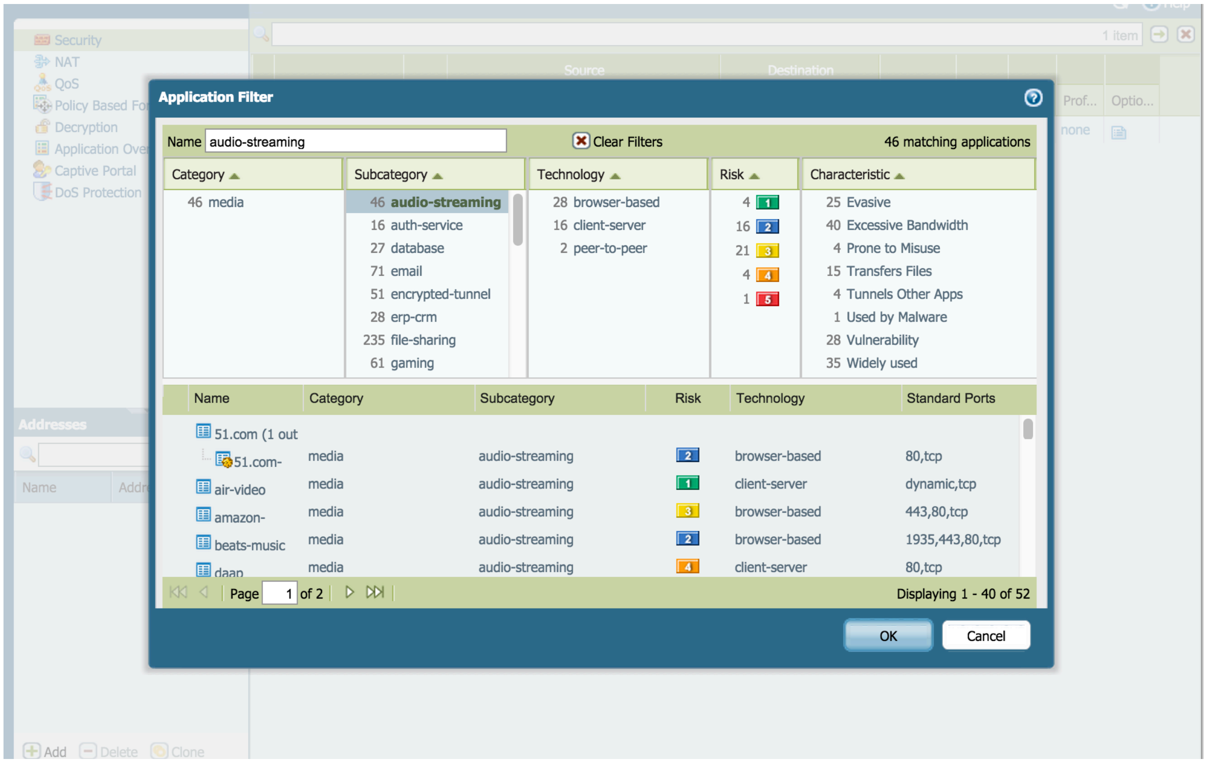
☑ Any

☐ Destination Address

☐ Negate

Figure 26. Setting the destination security zone

Under the Application tab, the audio-streaming category was set. By clicking Add > Application Filter, the entire “audio-streaming” category was added to rule (Figure 27). The Application settings were then verified (Figure 28).



Name: audio-streaming

46 matching applications

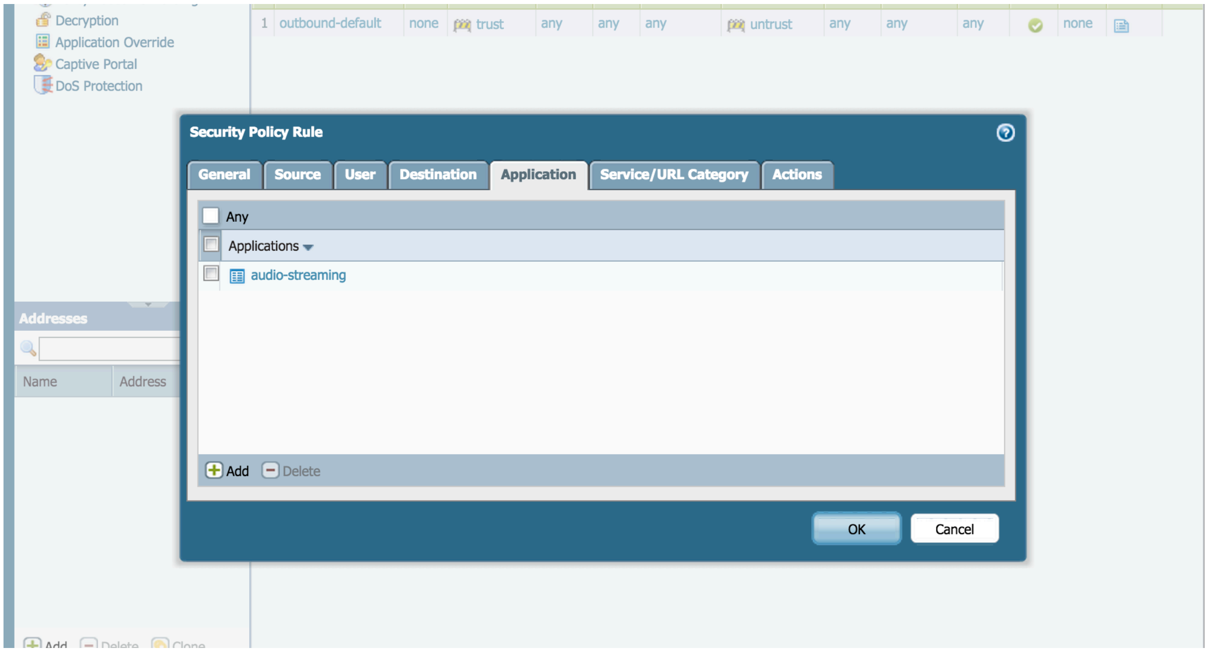
Category	Subcategory	Technology	Risk	Characteristic
46 media	46 audio-streaming	28 browser-based	4 1	25 Evasive
	16 auth-service	16 client-server	16 2	40 Excessive Bandwidth
	27 database	2 peer-to-peer	21 3	4 Prone to Misuse
	71 email		4 4	15 Transfers Files
	51 encrypted-tunnel		1 5	4 Tunnels Other Apps
	28 erp-crm			1 Used by Malware
	235 file-sharing			28 Vulnerability
	61 gaming			35 Widely used

Name	Category	Subcategory	Risk	Technology	Standard Ports
51.com (1 out					
51.com-	media	audio-streaming	2	browser-based	80,tcp
air-video	media	audio-streaming	1	client-server	dynamic,tcp
amazon-	media	audio-streaming	3	browser-based	443,80,tcp
beats-music	media	audio-streaming	2	browser-based	1935,443,80,tcp
daap	media	audio-streaming	4	client-server	80,tcp

Page 1 of 2

Displaying 1 - 40 of 52

Figure 27. Creating the application category filter for audio-streaming



1	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

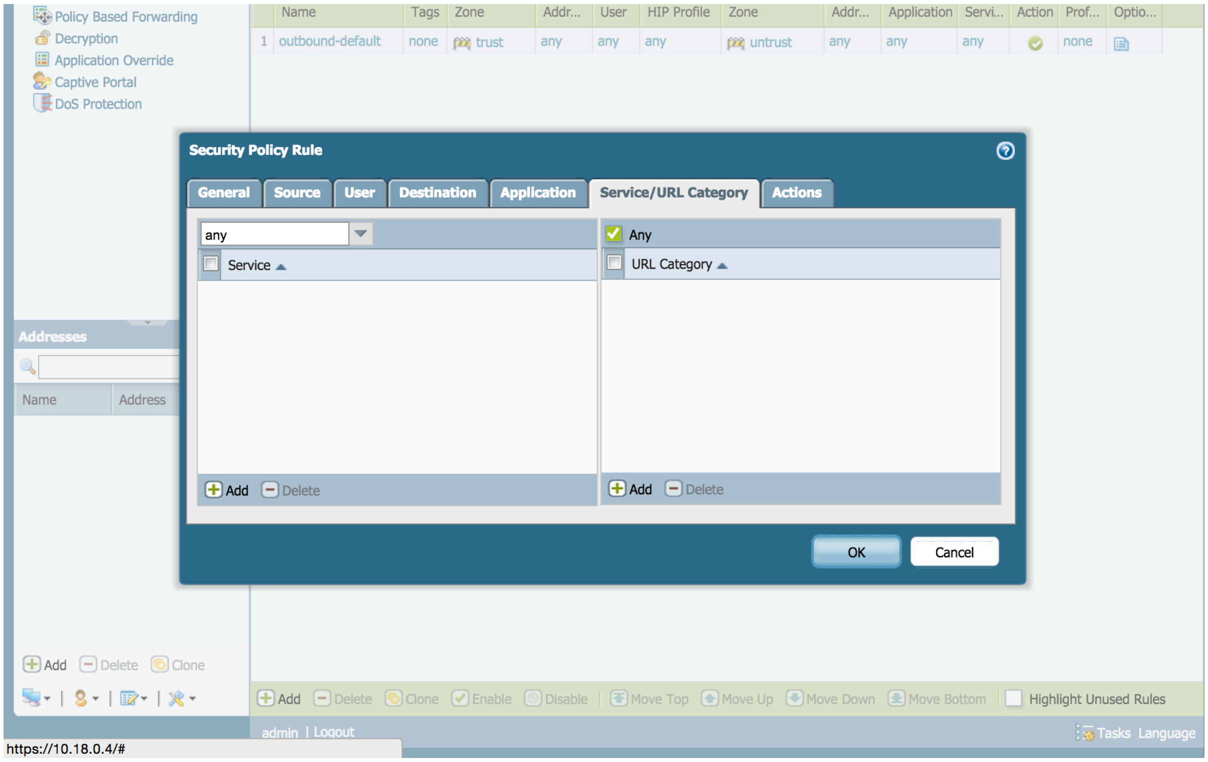
□ Any

□ Applications

□ audio-streaming

Figure 28. Confirming the Application tab is correct

The Service and URL Category are set to "any" (Figure 29).



	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

any

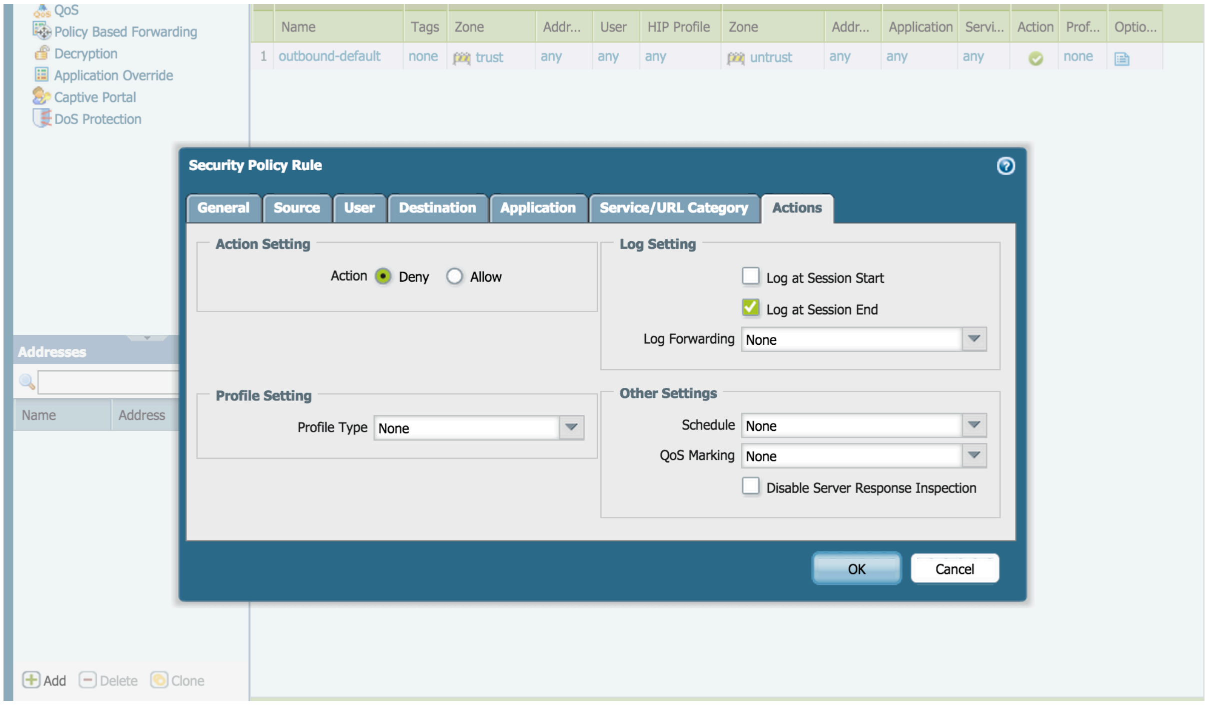
□ Service

☑ Any

□ URL Category

Figure 29. Setting the Service/URL options to "Any"

Under the Actions > Action Setting tab, the rule was set to "deny" to block matching traffic (Figure 30).



	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

Security Policy Rule

Action Setting

Action ● Deny ○ Allow

Log Setting

□ Log at Session Start

☑ Log at Session End

Log Forwarding None

Profile Setting

Profile Type None

Other Settings

Schedule None

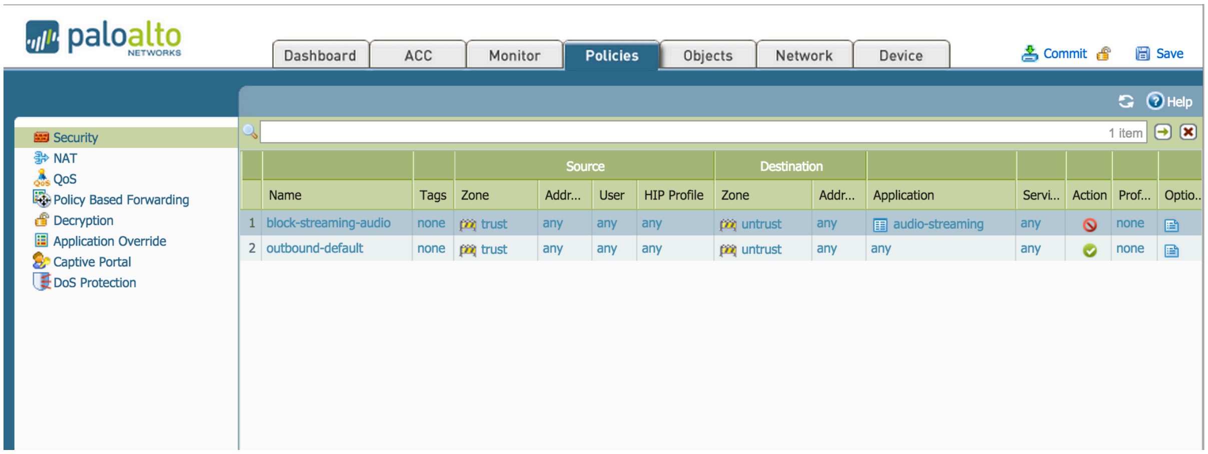
QoS Marking None

□ Disable Server Response Inspection

Name	Address

Figure 30. Setting the Action Setting to "Deny"

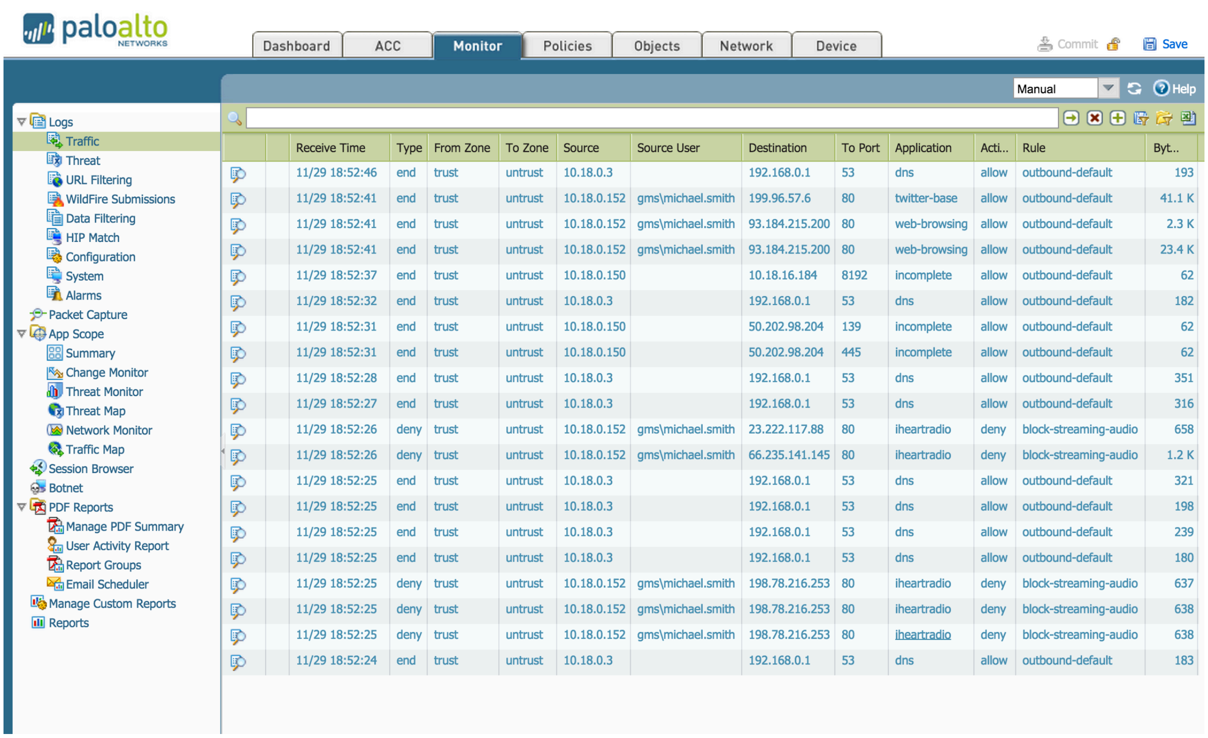
The rule was added and moved to the top so it would be enforced first (Figure 31).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	🚫	none	
2	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

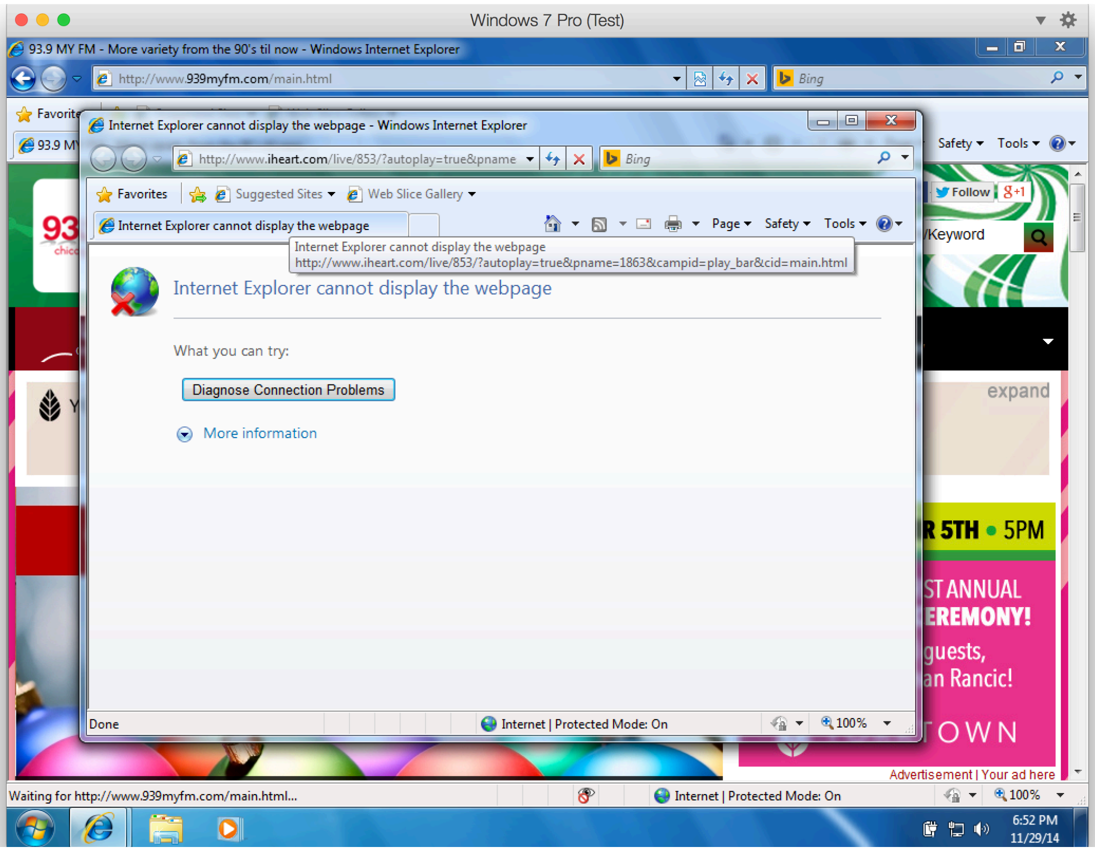
Figure 31. Confirming rule creation and order

By looking in the traffic logs, the rule was verified as working correctly (Figure 32). Student "michael.smith" attempted to load a streaming audio application and was denied. The user received a "Cannot Display Page" error when trying to load the page (Figure 33).



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/29 18:52:46	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	193
11/29 18:52:41	end	trust	untrust	10.18.0.152	gms\michael.smith	199.96.57.6	80	twitter-base	allow	outbound-default	41.1 K
11/29 18:52:41	end	trust	untrust	10.18.0.152	gms\michael.smith	93.184.215.200	80	web-browsing	allow	outbound-default	2.3 K
11/29 18:52:41	end	trust	untrust	10.18.0.152	gms\michael.smith	93.184.215.200	80	web-browsing	allow	outbound-default	23.4 K
11/29 18:52:37	end	trust	untrust	10.18.0.150		10.18.16.184	8192	incomplete	allow	outbound-default	62
11/29 18:52:32	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	182
11/29 18:52:31	end	trust	untrust	10.18.0.150		50.202.98.204	139	incomplete	allow	outbound-default	62
11/29 18:52:31	end	trust	untrust	10.18.0.150		50.202.98.204	445	incomplete	allow	outbound-default	62
11/29 18:52:28	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	351
11/29 18:52:27	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	316
11/29 18:52:26	deny	trust	untrust	10.18.0.152	gms\michael.smith	23.222.117.88	80	iheartradio	deny	block-streaming-audio	658
11/29 18:52:26	deny	trust	untrust	10.18.0.152	gms\michael.smith	66.235.141.145	80	iheartradio	deny	block-streaming-audio	1.2 K
11/29 18:52:25	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	321
11/29 18:52:25	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	198
11/29 18:52:25	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	239
11/29 18:52:25	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	180
11/29 18:52:25	deny	trust	untrust	10.18.0.152	gms\michael.smith	198.78.216.253	80	iheartradio	deny	block-streaming-audio	637
11/29 18:52:25	deny	trust	untrust	10.18.0.152	gms\michael.smith	198.78.216.253	80	iheartradio	deny	block-streaming-audio	638
11/29 18:52:25	deny	trust	untrust	10.18.0.152	gms\michael.smith	198.78.216.253	80	iheartradio	deny	block-streaming-audio	638
11/29 18:52:24	end	trust	untrust	10.18.0.3		192.168.0.1	53	dns	allow	outbound-default	183

Figure 32. Reviewing the traffic logs for blocked streaming audio traffic



Windows 7 Pro (Test)

93.9 MY FM - More variety from the 90's til now - Windows Internet Explorer

http://www.939myfm.com/main.html

Internet Explorer cannot display the webpage - Windows Internet Explorer

http://www.iheart.com/live/853/?autoplay=true&pname

Internet Explorer cannot display the webpage
http://www.iheart.com/live/853/?autoplay=true&pname=1863&campid=play_bar&cid=main.html

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems

More information

Done

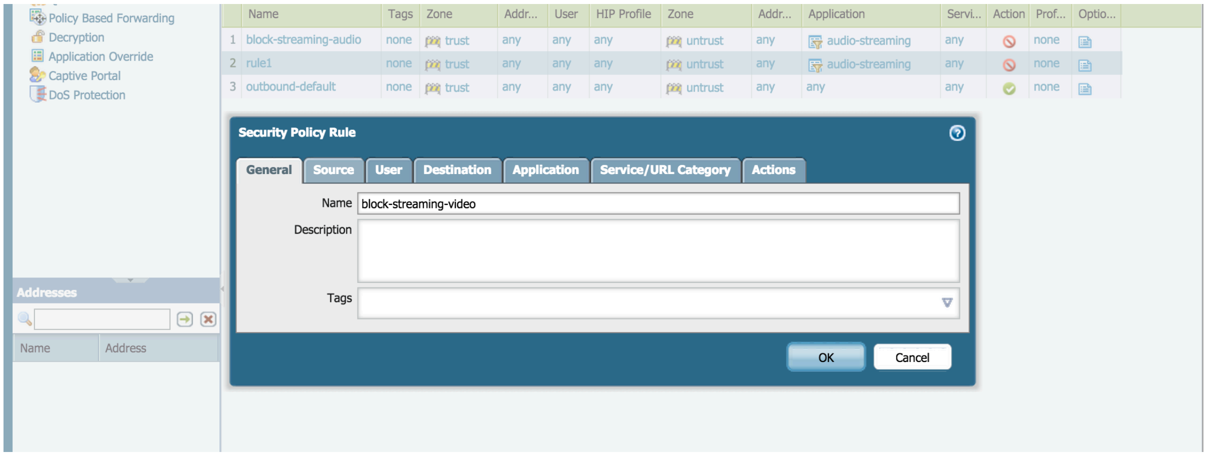
Internet | Protected Mode: On

Waiting for http://www.939myfm.com/main.html...

Figure 33. User's screen showing page load error

4.4 Creating the Streaming Video Rules

The next policy needed was to block streaming video for all users except staff. To enforce this policy, two security rules were created. When creating rules, similar rules can be cloned, creating a working copy. The working copy rule is then updated with needed changes and renamed. After cloning the "block-streaming-audio" rule, the appropriate changes were made. The rule was named "block-streaming-video" (Figure 34).



	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⃠	none	
2	rule1	none	trust	any	any	any	untrust	any	audio-streaming	any	⃠	none	
3	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

Security Policy Rule

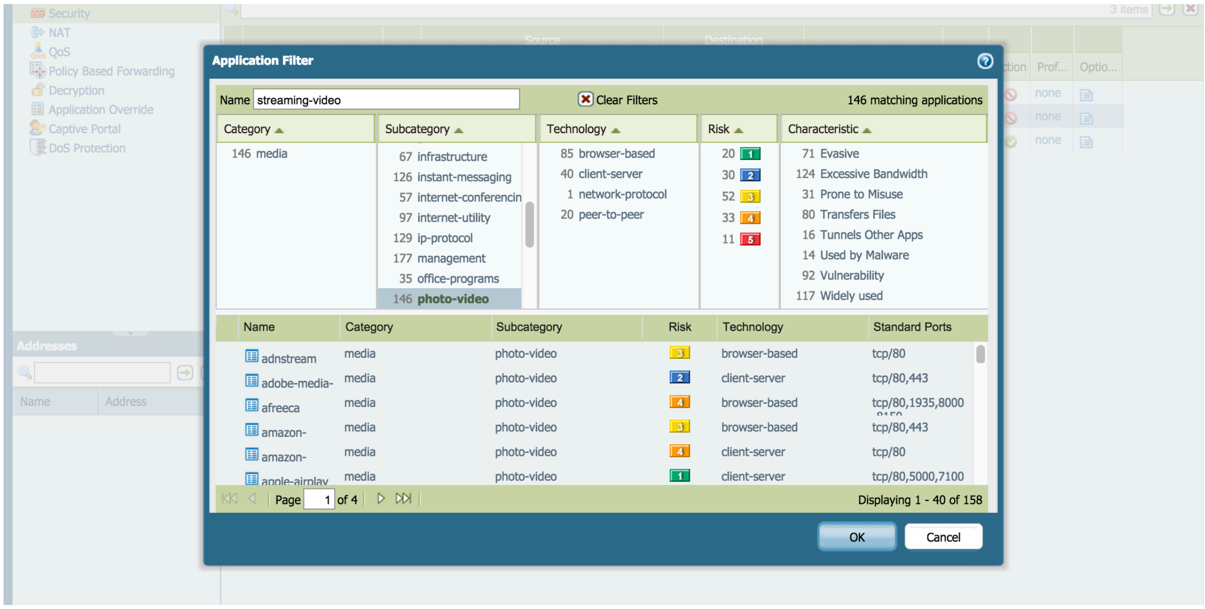
Name: block-streaming-video

Description:

Tags:

Figure 34. Naming the security rule "block-streaming-video"

Palo Alto categorizes streaming video application under the "photo-video" application category. In Figure 35, the application filter was created, named and added to the rule.



Name streaming-video ☒ Clear Filters 146 matching applications

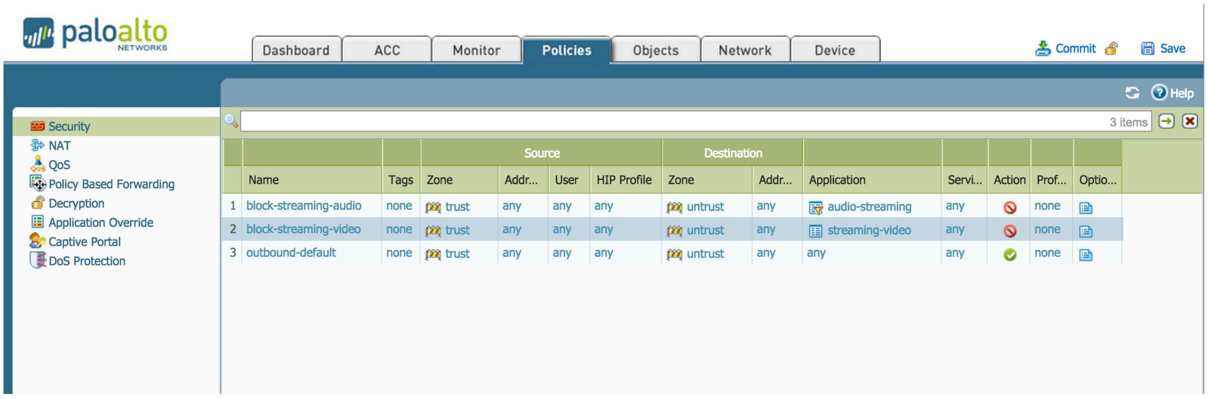
Category	Subcategory	Technology	Risk	Characteristic
146 media	67 infrastructure	85 browser-based	20 1	71 Evasive
	126 instant-messaging	40 client-server	30 2	124 Excessive Bandwidth
	57 internet-conferencin	1 network-protocol	52 3	31 Prone to Misuse
	97 internet-utility	20 peer-to-peer	33 4	80 Transfers Files
	129 ip-protocol		11 5	16 Tunnels Other Apps
	177 management			14 Used by Malware
	35 office-programs			92 Vulnerability
	146 photo-video			117 Widely used

Name	Category	Subcategory	Risk	Technology	Standard Ports
adnstream	media	photo-video	3	browser-based	tcp/80
adobe-media-	media	photo-video	2	client-server	tcp/80,443
afreeca	media	photo-video	4	browser-based	tcp/80,1935,8000
amazon-	media	photo-video	3	browser-based	tcp/80,443
amazon-	media	photo-video	4	client-server	tcp/80
apple-airplay	media	photo-video	1	client-server	tcp/80,5000,7100

Page 1 of 4 Displaying 1 - 40 of 158

Figure 35. Creating the application category filter for "streaming-video"

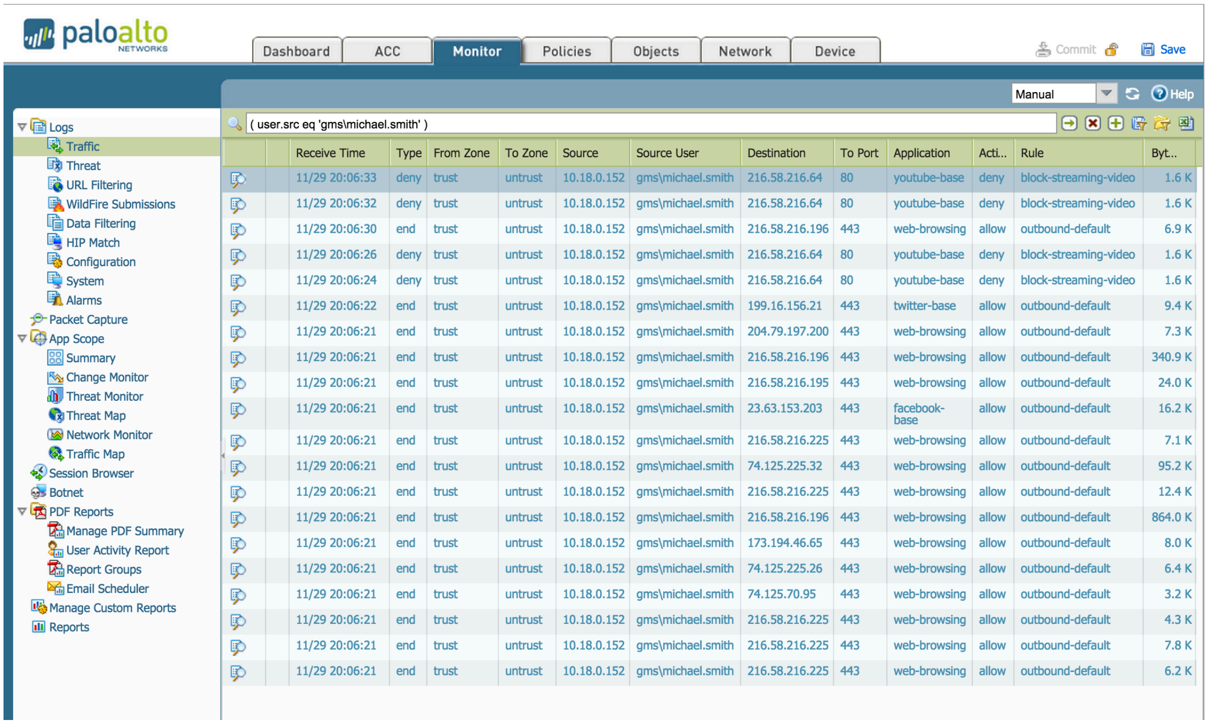
The rule was added and configuration changes were saved (Figure 36).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	
2	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
3	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

Figure 36. Confirming the rule creation and order

By looking in the traffic logs, the rule was verified as working correctly (Figure 37). Student "michael.smith" attempted to load a streaming YouTube video and was denied.

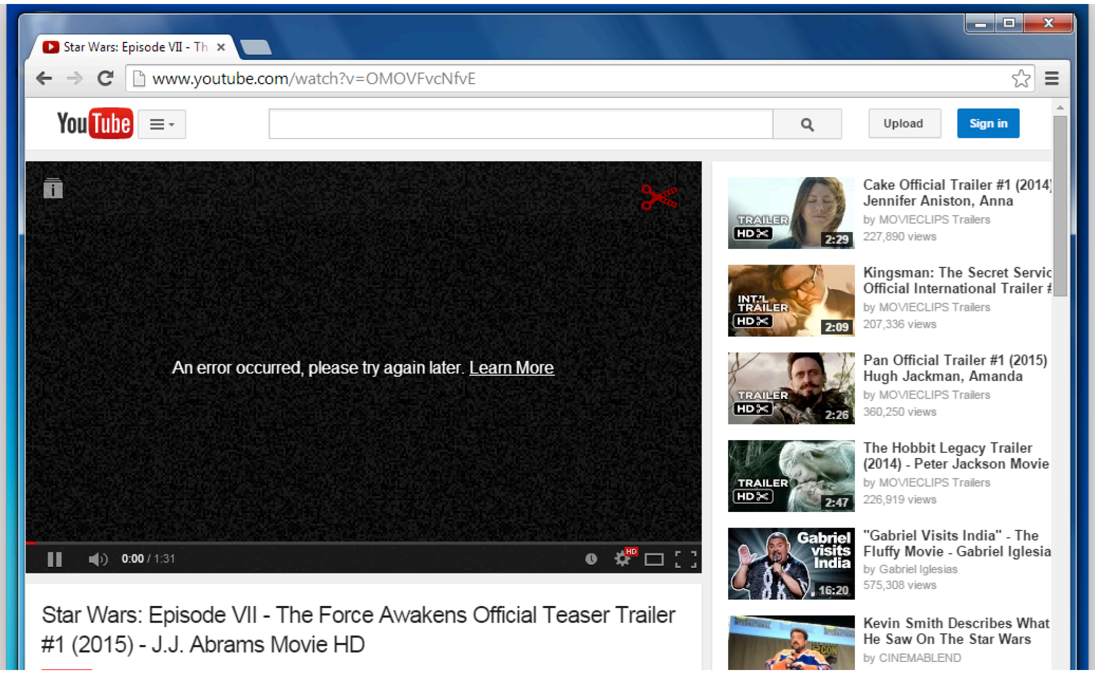


(user.src eq 'gms\michael.smith')

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/29 20:06:33	deny	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.64	80	youtube-base	deny	block-streaming-video	1.6 K
11/29 20:06:32	deny	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.64	80	youtube-base	deny	block-streaming-video	1.6 K
11/29 20:06:30	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.196	443	web-browsing	allow	outbound-default	6.9 K
11/29 20:06:26	deny	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.64	80	youtube-base	deny	block-streaming-video	1.6 K
11/29 20:06:24	deny	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.64	80	youtube-base	deny	block-streaming-video	1.6 K
11/29 20:06:22	end	trust	untrust	10.18.0.152	gms\michael.smith	199.16.156.21	443	twitter-base	allow	outbound-default	9.4 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	204.79.197.200	443	web-browsing	allow	outbound-default	7.3 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.196	443	web-browsing	allow	outbound-default	340.9 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.195	443	web-browsing	allow	outbound-default	24.0 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	23.63.153.203	443	facebook-base	allow	outbound-default	16.2 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.225	443	web-browsing	allow	outbound-default	7.1 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.32	443	web-browsing	allow	outbound-default	95.2 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.225	443	web-browsing	allow	outbound-default	12.4 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.196	443	web-browsing	allow	outbound-default	864.0 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	173.194.46.65	443	web-browsing	allow	outbound-default	8.0 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.26	443	web-browsing	allow	outbound-default	6.4 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.70.95	443	web-browsing	allow	outbound-default	3.2 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.225	443	web-browsing	allow	outbound-default	4.3 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.225	443	web-browsing	allow	outbound-default	7.8 K
11/29 20:06:21	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.225	443	web-browsing	allow	outbound-default	6.2 K

Figure 37. Reviewing the traffic logs for blocked streaming video traffic

The user “michael.smith” received an “Error Occurred” message in the video window when trying to load the page (Figure 38).

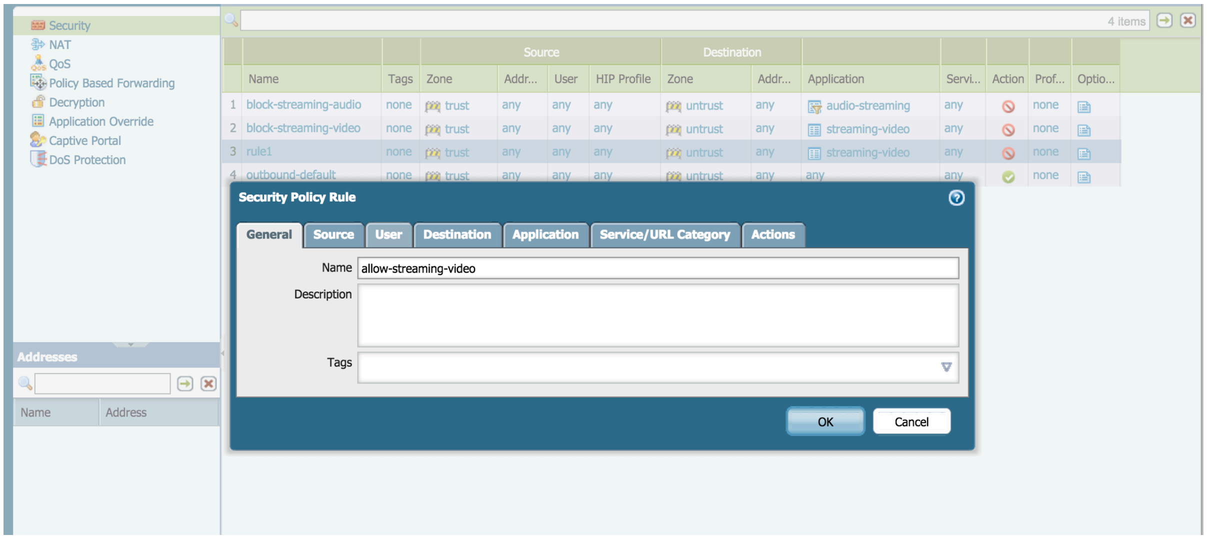

Star Wars: Episode VII - Th
www.youtube.com/watch?v=OMOVFvcNfvE
YouTube
Upload
Sign in
0:00 / 1:31
Cake Official Trailer #1 (2014)
Jennifer Aniston, Anna
by MOVIECLIPS Trailers
227,890 views
2:29
Kingsman: The Secret Servic
Official International Trailer #
by MOVIECLIPS Trailers
207,336 views
2:09
Pan Official Trailer #1 (2015)
Hugh Jackman, Amanda
by MOVIECLIPS Trailers
360,250 views
2:26
The Hobbit Legacy Trailer
(2014) - Peter Jackson Movie
by MOVIECLIPS Trailers
226,919 views
2:47
"Gabriel Visits India" - The
Fluffy Movie - Gabriel Iglesia
by Gabriel Iglesias
575,308 views
16:20
Kevin Smith Describes What
He Saw On The Star Wars
by CINEMABLEND

An error occurred, please try again later. Learn More

Star Wars: Episode VII - The Force Awakens Official Teaser Trailer #1 (2015) - J.J. Abrams Movie HD

Figure 38. User’s screen showing video loading error

Next the second rule was made to allow staff access to streaming video. The “block-streaming-video” rule was cloned. The rule was renamed “allow-streaming-video” (Figure 39).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	
2	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
3	rule1	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
4	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

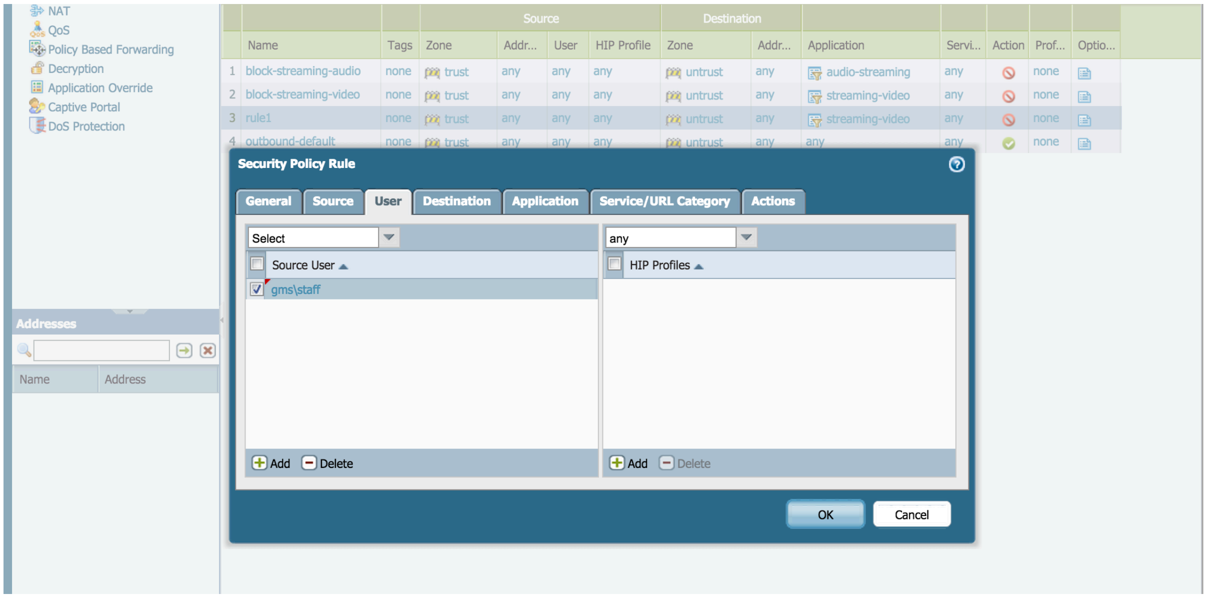
Name: allow-streaming-video

Description:

Tags:

Figure 39. Naming the “allow-streaming-video” rule

Next, the User tab was updated to include the “gms\staff” group from the directory server (Figure 40).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	
2	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
3	rule1	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
4	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

Select

□ Source User ▲

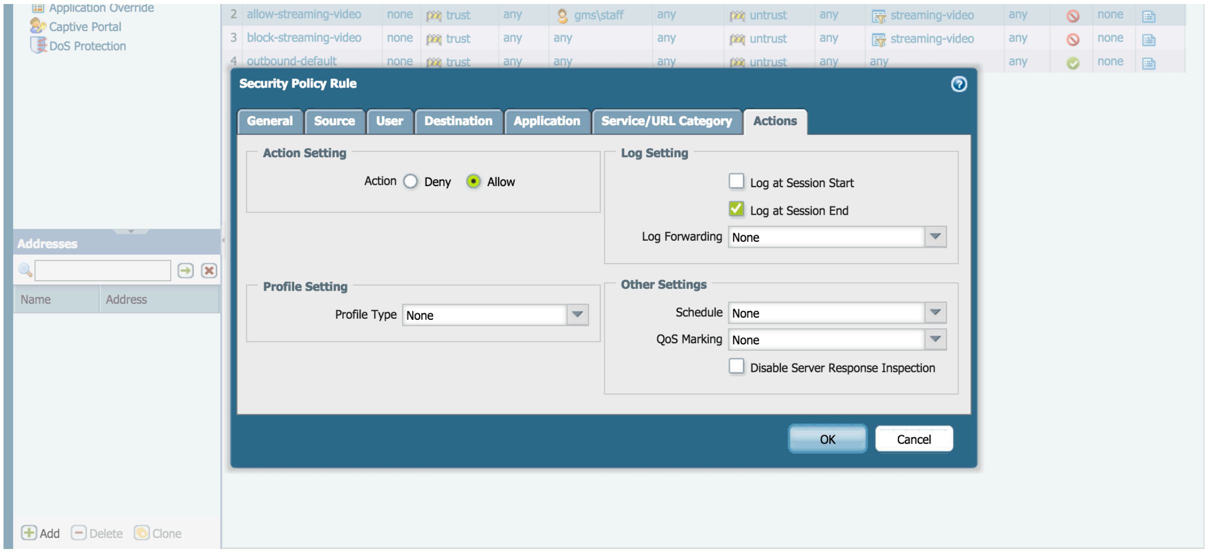
☑ gms\staff

any

□ HIP Profiles ▲

Figure 40. Setting the source user to the “gms\staff” group

Lastly, the Action tab was updated. The Action Setting was changed from “Deny” to “Allow” (Figure 41). The rule was added and moved to the top (Figure 42).



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action ○ Deny ● Allow

Log Setting

☐ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

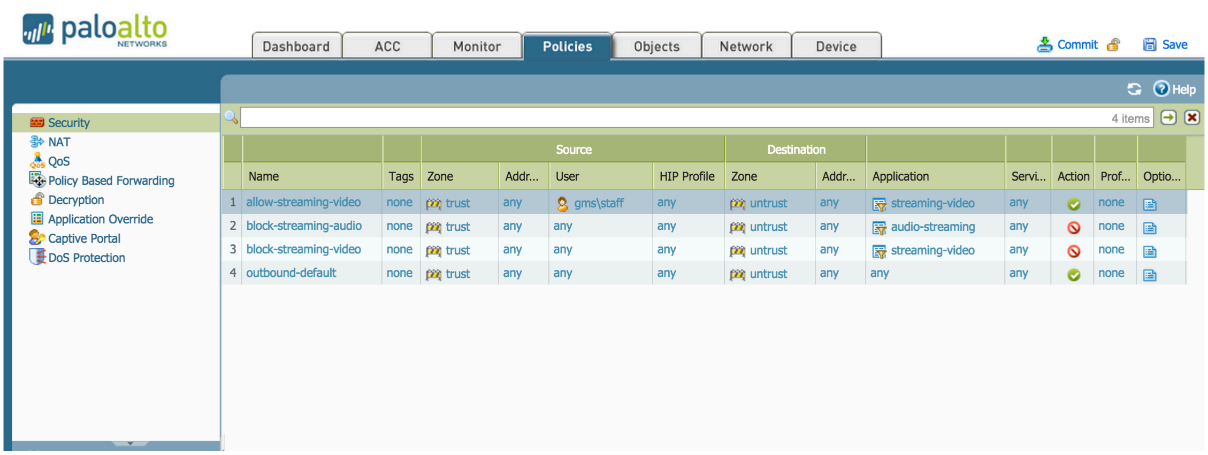
Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

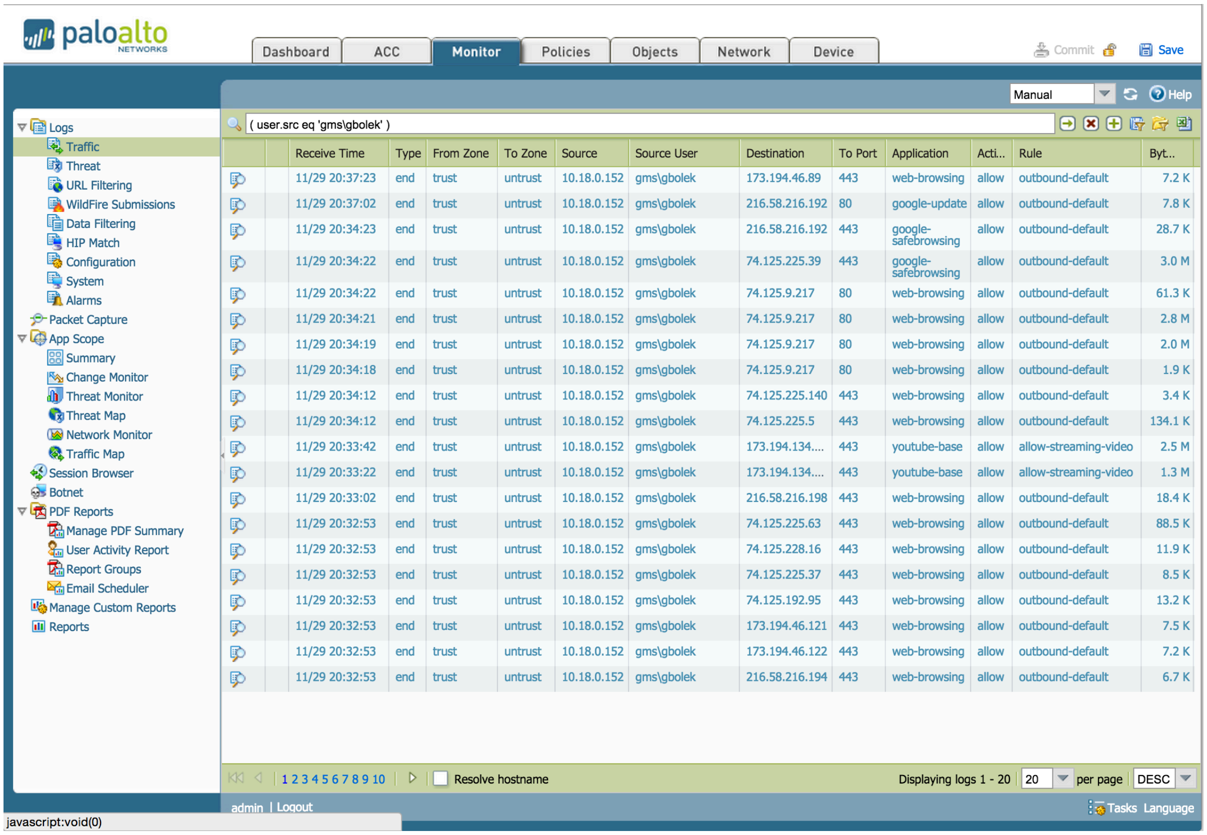
Figure 41. Changing the Action Setting to "Allow"



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	✓	none	
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	
4	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	none	

Figure 42. Confirming rule creation and order

By looking in the traffic logs, the rule was verified as working correctly (Figure 43). Staff "gbolek" attempted to load a streaming YouTube video and was successful.



(user.src eq 'gms\gbolek')

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/29 20:37:23	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.46.89	443	web-browsing	allow	outbound-default	7.2 K
11/29 20:37:02	end	trust	untrust	10.18.0.152	gms\gbolek	216.58.216.192	80	google-update	allow	outbound-default	7.8 K
11/29 20:34:23	end	trust	untrust	10.18.0.152	gms\gbolek	216.58.216.192	443	google-safebrowsing	allow	outbound-default	28.7 K
11/29 20:34:22	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.39	443	google-safebrowsing	allow	outbound-default	3.0 M
11/29 20:34:22	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.9.217	80	web-browsing	allow	outbound-default	61.3 K
11/29 20:34:21	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.9.217	80	web-browsing	allow	outbound-default	2.8 M
11/29 20:34:19	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.9.217	80	web-browsing	allow	outbound-default	2.0 M
11/29 20:34:18	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.9.217	80	web-browsing	allow	outbound-default	1.9 K
11/29 20:34:12	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.140	443	web-browsing	allow	outbound-default	3.4 K
11/29 20:34:12	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.5	443	web-browsing	allow	outbound-default	134.1 K
11/29 20:33:42	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.134....	443	youtube-base	allow	allow-streaming-video	2.5 M
11/29 20:33:22	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.134....	443	youtube-base	allow	allow-streaming-video	1.3 M
11/29 20:33:02	end	trust	untrust	10.18.0.152	gms\gbolek	216.58.216.198	443	web-browsing	allow	outbound-default	18.4 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.63	443	web-browsing	allow	outbound-default	88.5 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.228.16	443	web-browsing	allow	outbound-default	11.9 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.37	443	web-browsing	allow	outbound-default	8.5 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.192.95	443	web-browsing	allow	outbound-default	13.2 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.46.121	443	web-browsing	allow	outbound-default	7.5 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.46.122	443	web-browsing	allow	outbound-default	7.2 K
11/29 20:32:53	end	trust	untrust	10.18.0.152	gms\gbolek	216.58.216.194	443	web-browsing	allow	outbound-default	6.7 K

1 2 3 4 5 6 7 8 9 10 □ Resolve hostname Displaying logs 1 - 20 20 per page DESC

Figure 43. Reviewing the traffic logs for allowed streaming video

The user "gbolek" was able to view the video from YouTube (Figure 44).

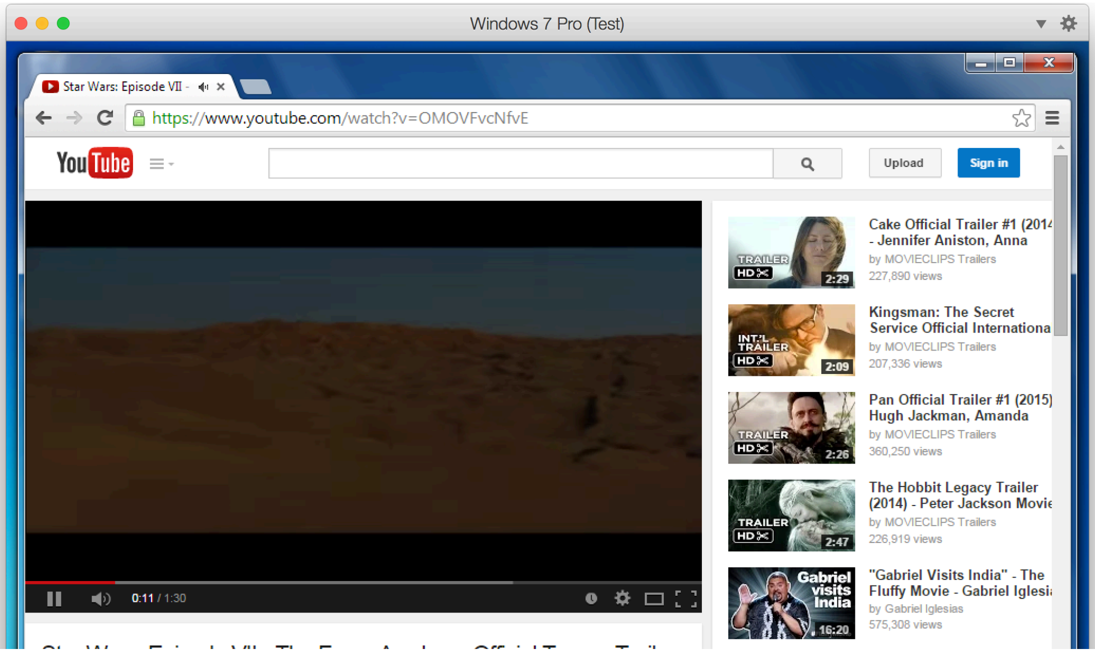
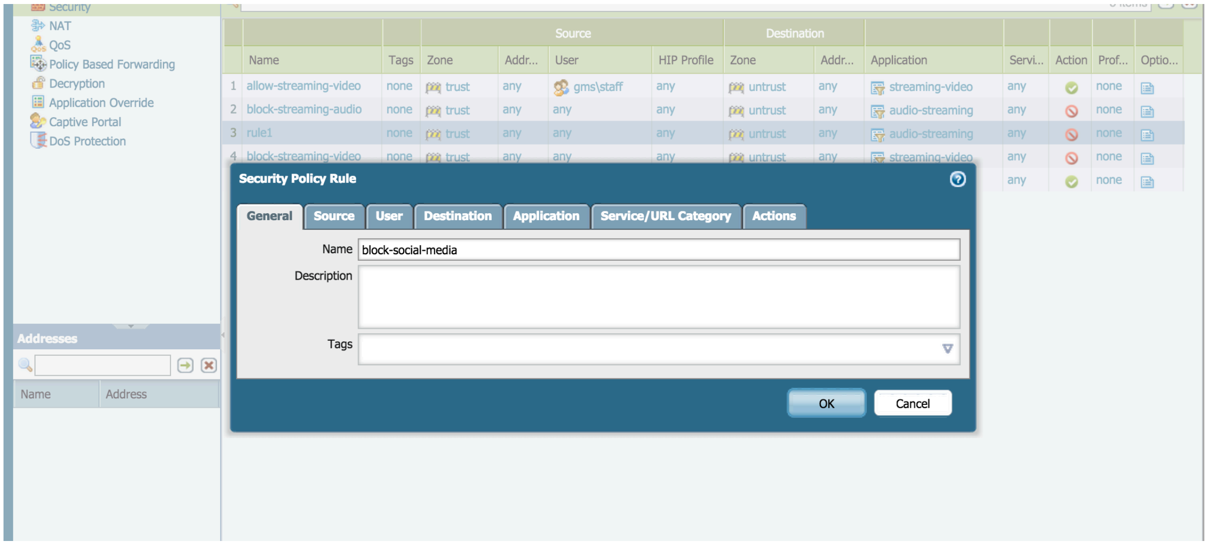

Windows 7 Pro (Test)
Star Wars: Episode VII -
https://www.youtube.com/watch?v=OMOVFvcNfvE
YouTube
Upload
Sign in
0:11 / 1:30
TRAILER HD 2:29
Cake Official Trailer #1 (2014 - Jennifer Aniston, Anna
by MOVIECLIPS Trailers
227,890 views
INT'L TRAILER HD 2:09
Kingsman: The Secret Service Official Internationa
by MOVIECLIPS Trailers
207,336 views
TRAILER HD 2:26
Pan Official Trailer #1 (2015) Hugh Jackman, Amanda
by MOVIECLIPS Trailers
360,250 views
TRAILER HD 2:47
The Hobbit Legacy Trailer (2014) - Peter Jackson Movie
by MOVIECLIPS Trailers
226,919 views
Gabriel visits India 16:20
"Gabriel Visits India" - The Fluffy Movie - Gabriel Iglesia
by Gabriel Iglesias
575,308 views

Figure 44. User successfully loads YouTube video

4.5 Creating the Social Media Rules

The last set of rules needed was to address social media. School administration decided all social media should be blocked, with the exception of Twitter. Twitter should be accessible for Principal Jones only. Implementation of this policy required use of App-ID, User-ID and Content-ID. Social media presents itself through both applications and web sites. App-ID was used to block the social media applications and the URL filtering of Content-ID was used to block the social media web sites.

First, the security rules were created for social media. The "block-streaming-audio" rule was cloned and renamed "block-social-media" (Figure 45).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	✓	none	
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⃠	none	
3	rule1	none	trust	any	any	any	untrust	any	audio-streaming	any	⃠	none	
4	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⃠	none	
										any	✓	none	

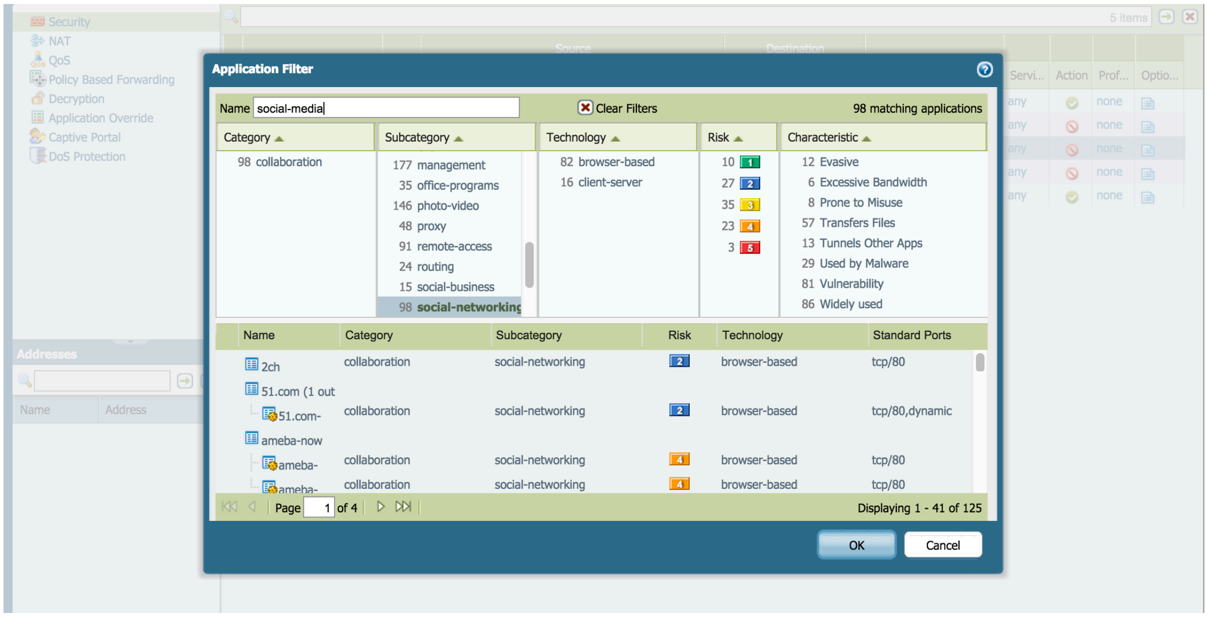
Name: block-social-media

Description:

Tags:

Figure 45. Naming the security rule "block-social-media"

Palo Alto categorizes social networking applications under the "social media" application category. In Figure 46, the application filter was created, named and added to the rule (Figure 47).



Name social-media

☒ Clear Filters

98 matching applications

Category ▲

- 98 collaboration

Subcategory ▲

- 177 management
- 35 office-programs
- 146 photo-video
- 48 proxy
- 91 remote-access
- 24 routing
- 15 social-business
- 98 social-networking

Technology ▲

- 82 browser-based
- 16 client-server

Risk ▲

- 10 1
- 27 2
- 35 3
- 23 4
- 3 5

Characteristic ▲

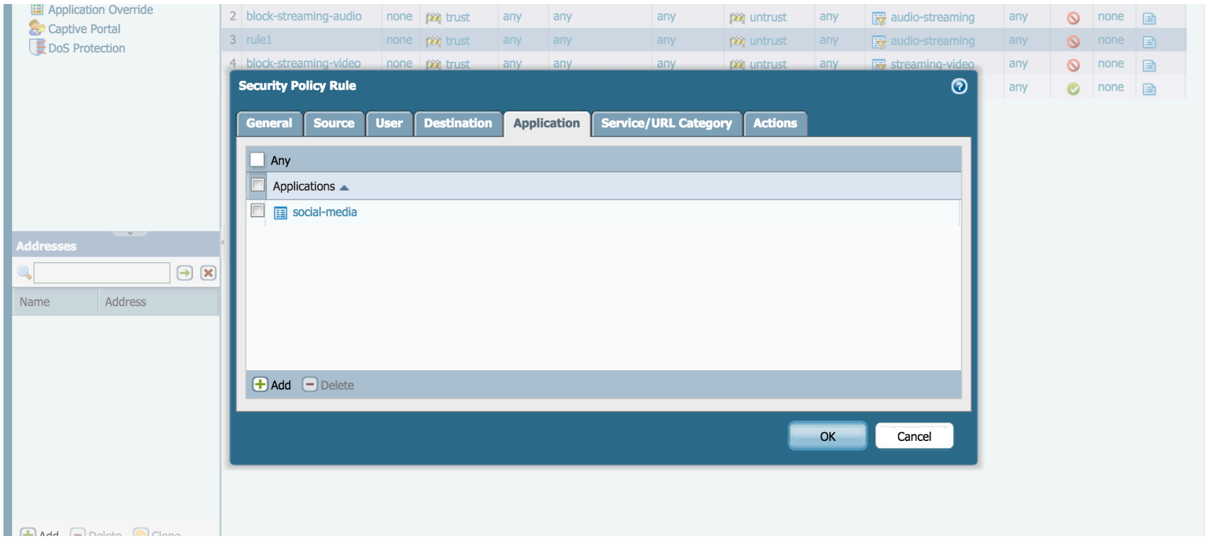
- 12 Evasive
- 6 Excessive Bandwidth
- 8 Prone to Misuse
- 57 Transfers Files
- 13 Tunnels Other Apps
- 29 Used by Malware
- 81 Vulnerability
- 86 Widely used

Name	Category	Subcategory	Risk	Technology	Standard Ports
2ch	collaboration	social-networking	2	browser-based	tcp/80
51.com (1 out					
51.com-	collaboration	social-networking	2	browser-based	tcp/80,dynamic
ameba-now					
ameba-	collaboration	social-networking	4	browser-based	tcp/80
ameba-	collaboration	social-networking	4	browser-based	tcp/80

Page 1 of 4

Displaying 1 - 41 of 125

Figure 46. Creating the application category filter



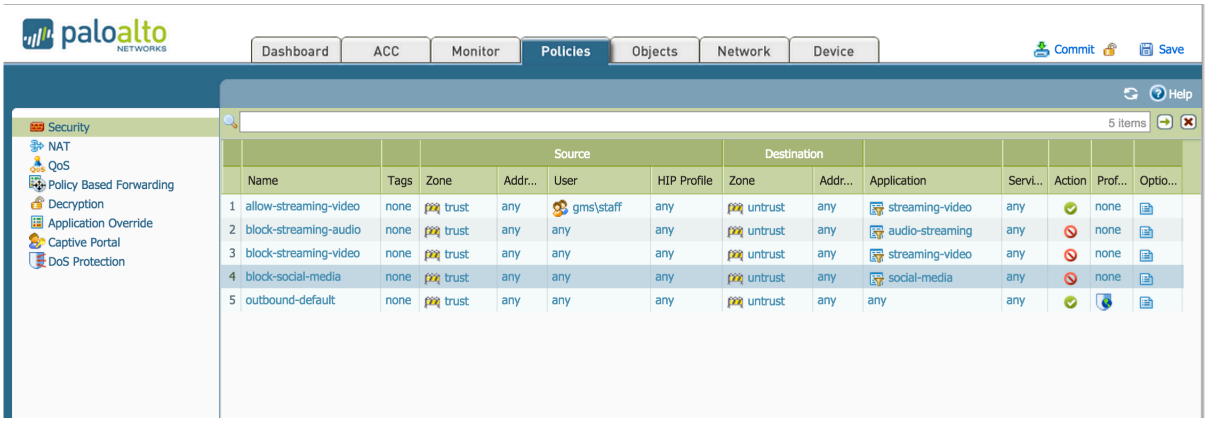
☐ Any

☐ Applications ▲

☐ social-media

Figure 47. Confirming Application tab settings

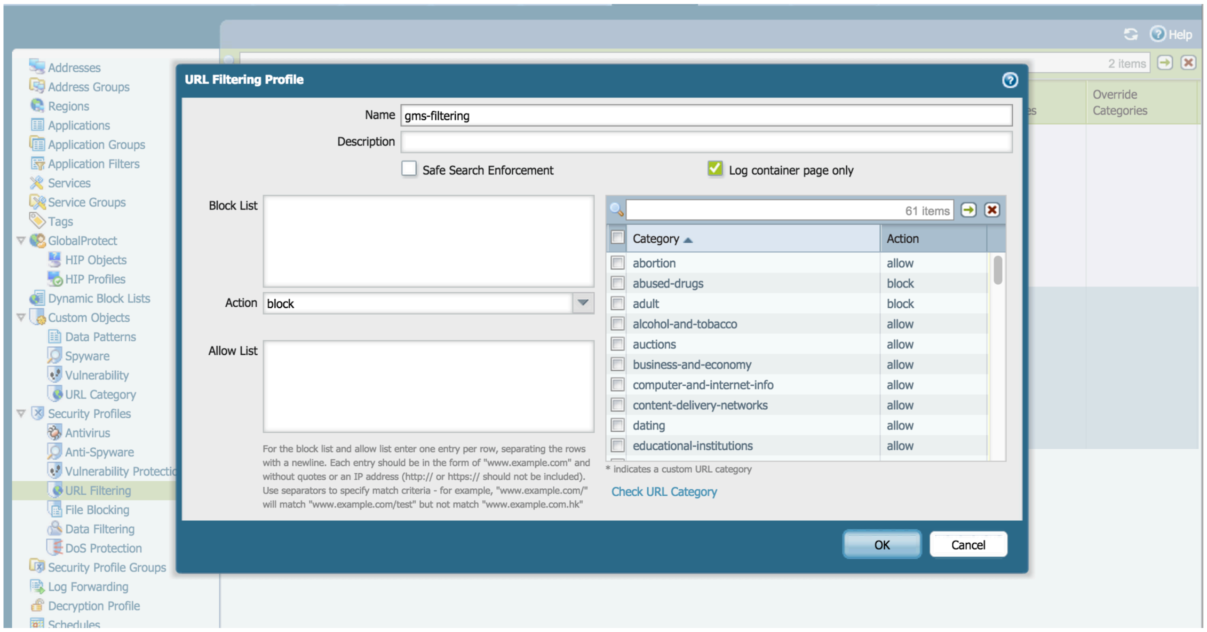
The rule was added and moved above the “outbound-default” (Figure 48).



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	✓	none	🗎
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	🗎
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	🗎
4	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	⊘	none	🗎
5	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	●	🗎

Figure 48. Confirming rule creation and order

Next, the URL filtering was setup. First, under Objects > Security Profiles > URL Filtering the "default" profile was cloned and named "gms-filtering" (Figure 49). This is the default filtering profile for all traffic.



Name gms-filtering

Description

☐ Safe Search Enforcement ☑ Log container page only

Block List

Action block

Allow List

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

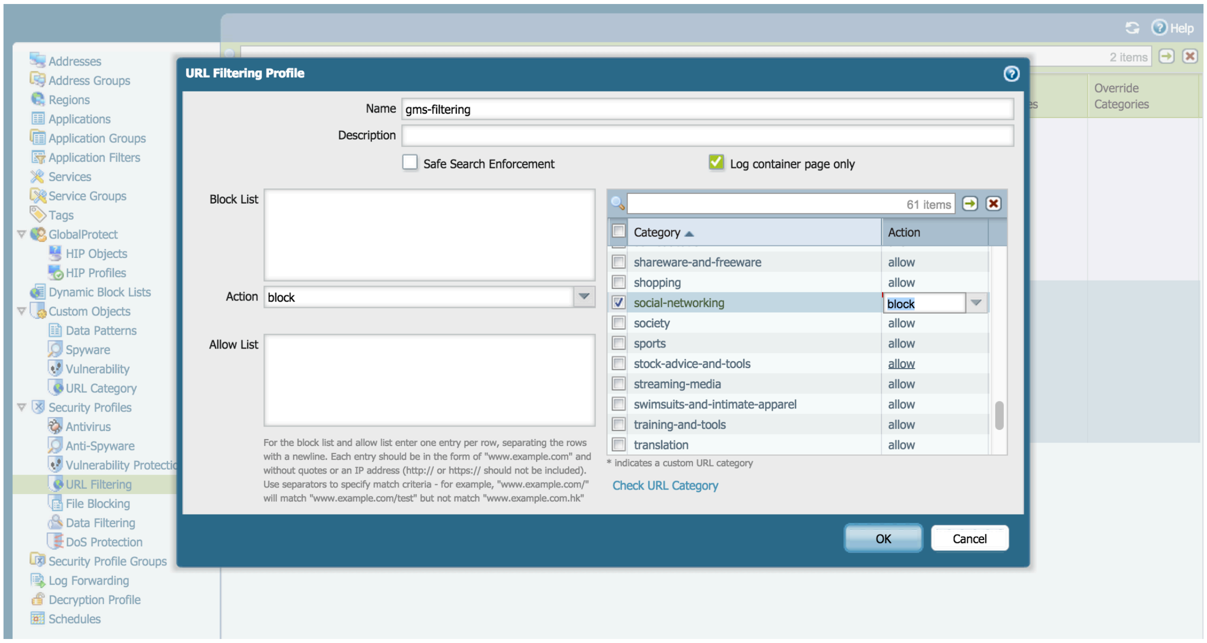
☐ Category ▲	Action
☐ abortion	allow
☐ abused-drugs	block
☐ adult	block
☐ alcohol-and-tobacco	allow
☐ auctions	allow
☐ business-and-economy	allow
☐ computer-and-internet-info	allow
☐ content-delivery-networks	allow
☐ dating	allow
☐ educational-institutions	allow

* indicates a custom URL category

Check URL Category

Figure 49. Creating a URL Filtering profile

Next, the "social-networking" category was updated from "allow" to "block" (Figure 50). This will block all URL's categorized as social media (Figure 51).



Name gms-filtering

Description

☐ Safe Search Enforcement ☑ Log container page only

Block List

Action block

Allow List

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

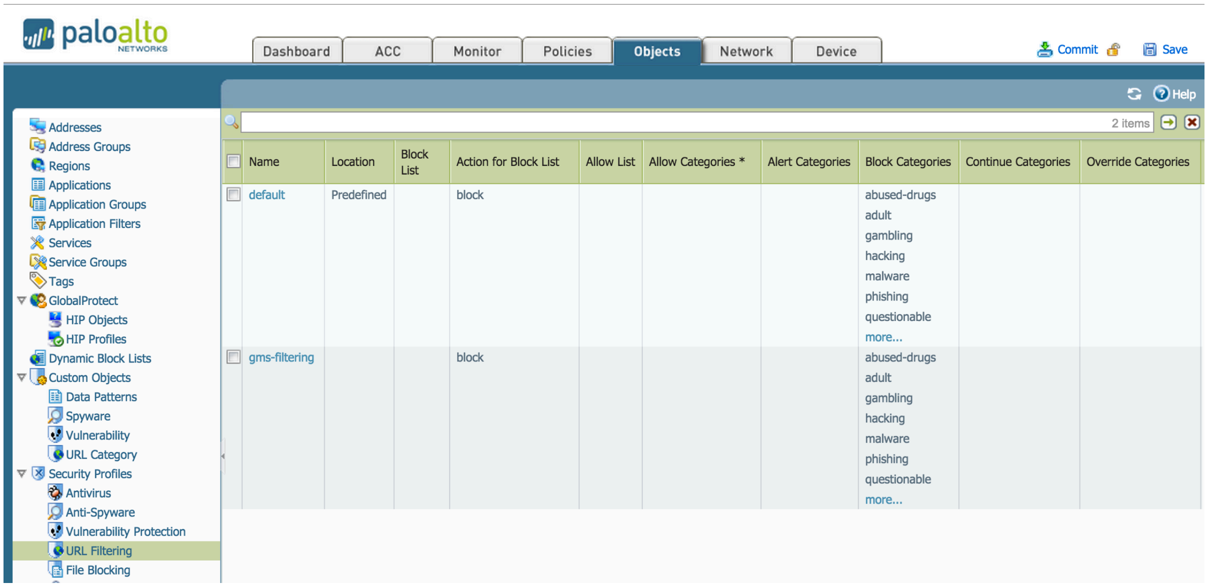
61 items

☐ Category ▲	Action
☐ shareware-and-freeware	allow
☐ shopping	allow
☑ social-networking	block
☐ society	allow
☐ sports	allow
☐ stock-advice-and-tools	allow
☐ streaming-media	allow
☐ swimsuits-and-intimate-apparel	allow
☐ training-and-tools	allow
☐ translation	allow

* indicates a custom URL category

Check URL Category

Figure 50. Changing the default settings for social-networking to "block"

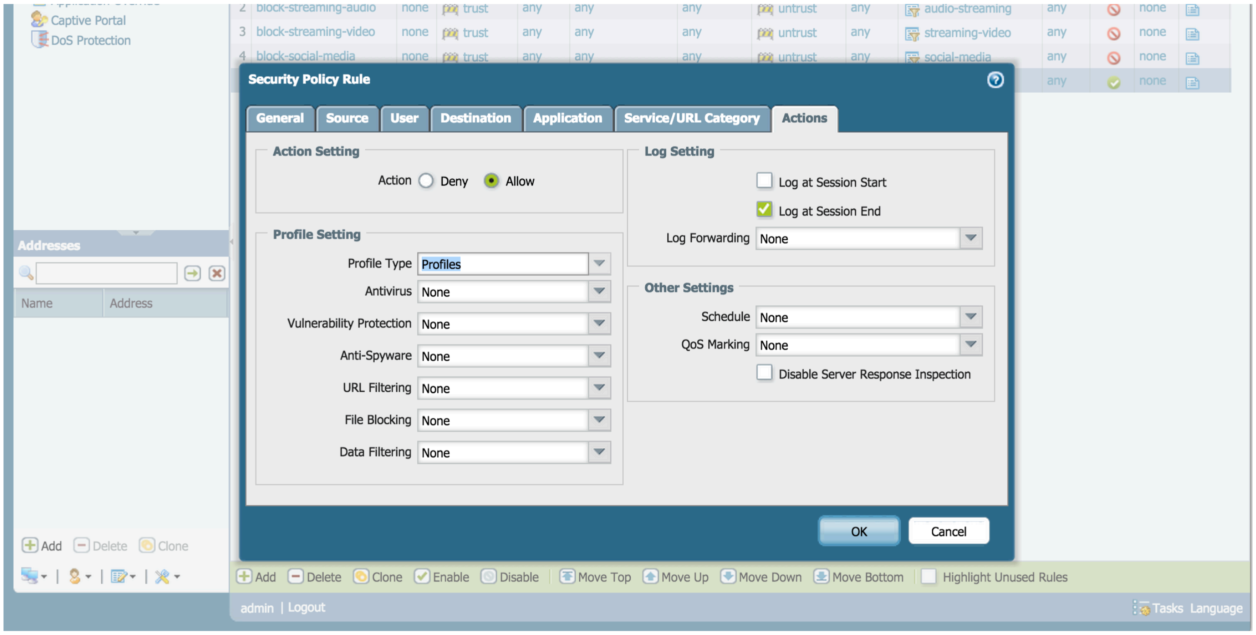


2 items

☐ Name	Location	Block List	Action for Block List	Allow List	Allow Categories *	Alert Categories	Block Categories	Continue Categories	Override Categories
☐ default	Predefined		block				abused-drugs adult gambling hacking malware phishing questionable more...		
☐ gms-filtering			block				abused-drugs adult gambling hacking malware phishing questionable more...		

Figure 51. Confirming profile creation

Finally, this profile was setup on the "outbound-default" rule. This enforces the URL filtering profile on all outbound traffic that does not match any preceding rules. Under Actions > Profiles > Profile Type, the option was changed to "Profiles" (Figure 52).



2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	none
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	none
4	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	none

Security Policy Rule

Action Setting

Action ○ Deny ● Allow

Profile Setting

Profile Type: Profiles
Antivirus: None
Vulnerability Protection: None
Anti-Spyware: None
URL Filtering: None
File Blocking: None
Data Filtering: None

Log Setting

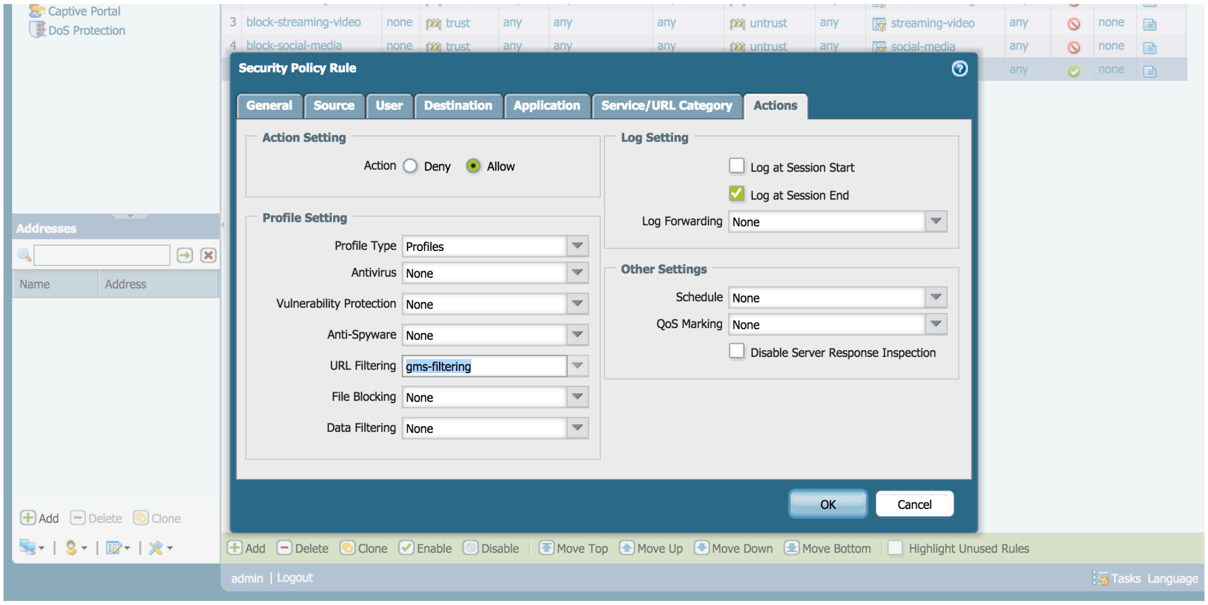
□ Log at Session Start
☑ Log at Session End
Log Forwarding: None

Other Settings

Schedule: None
QoS Marking: None
□ Disable Server Response Inspection

Figure 52. Changing the profile settings for the default-outbound rule

Then under URL Filtering, the option was changed to "gms-filtering" (Figure 53) and verified (Figure 54). Under the profile column the "shield" icon was now visible.



3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	none
4	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	none

Security Policy Rule

Action Setting

Action ○ Deny ● Allow

Profile Setting

Profile Type: Profiles
Antivirus: None
Vulnerability Protection: None
Anti-Spyware: None
URL Filtering: gms-filtering
File Blocking: None
Data Filtering: None

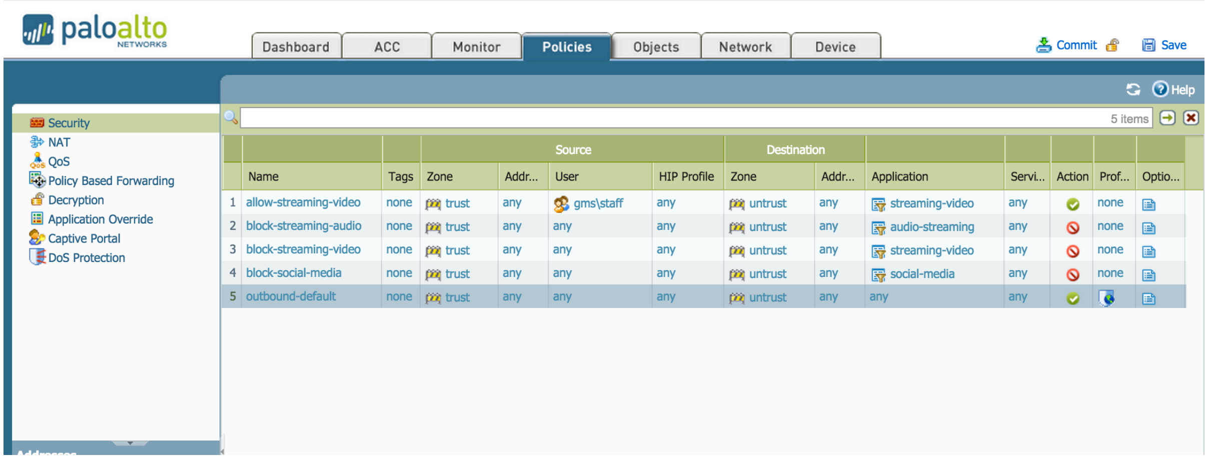
Log Setting

□ Log at Session Start
☑ Log at Session End
Log Forwarding: None

Other Settings

Schedule: None
QoS Marking: None
□ Disable Server Response Inspection

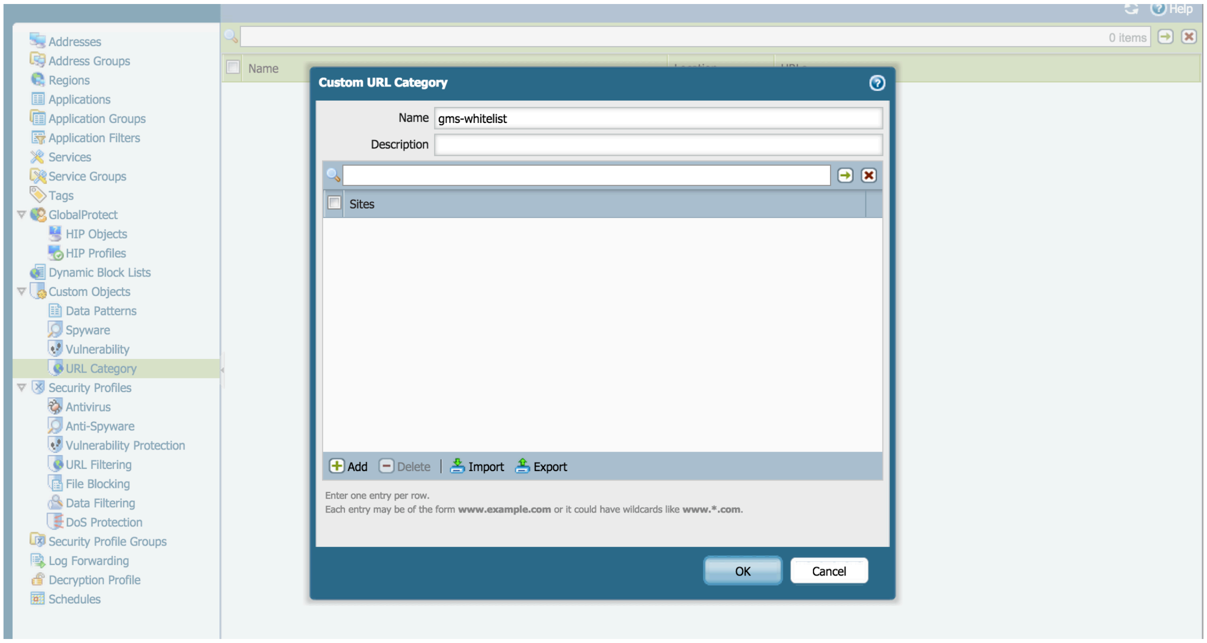
Figure 53. Applying the URL Filtering profile



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	✓	none	▤
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	▤
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	▤
4	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	⊘	none	▤
5	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓		▤

Figure 54. Confirming the URL Profile settings

Finally, the Twitter exception for Principal Jones was created. Under Objects > Custom Objects > URL Category, the whitelist was created and named "gms-whitelist" (Figure 55).



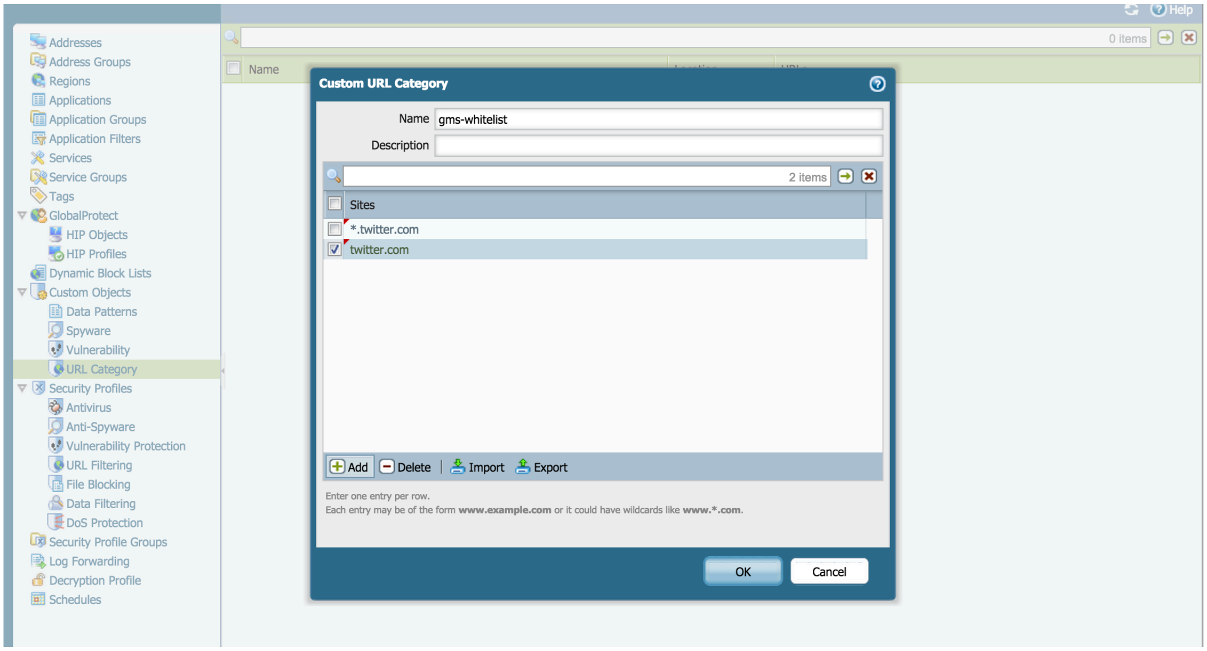
Name: gms-whitelist

Description:

Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

Figure 55. Creating the custom URL category

Then the Twitter domain was added to the whitelist (Figure 56). Palo Alto's recommendation is sites are added to custom URL lists in the following manner, one entry for the root domain and a second entry for all subdomains. This ensures the URL's are filtered properly.



Custom URL Category

Name: gms-whitelist

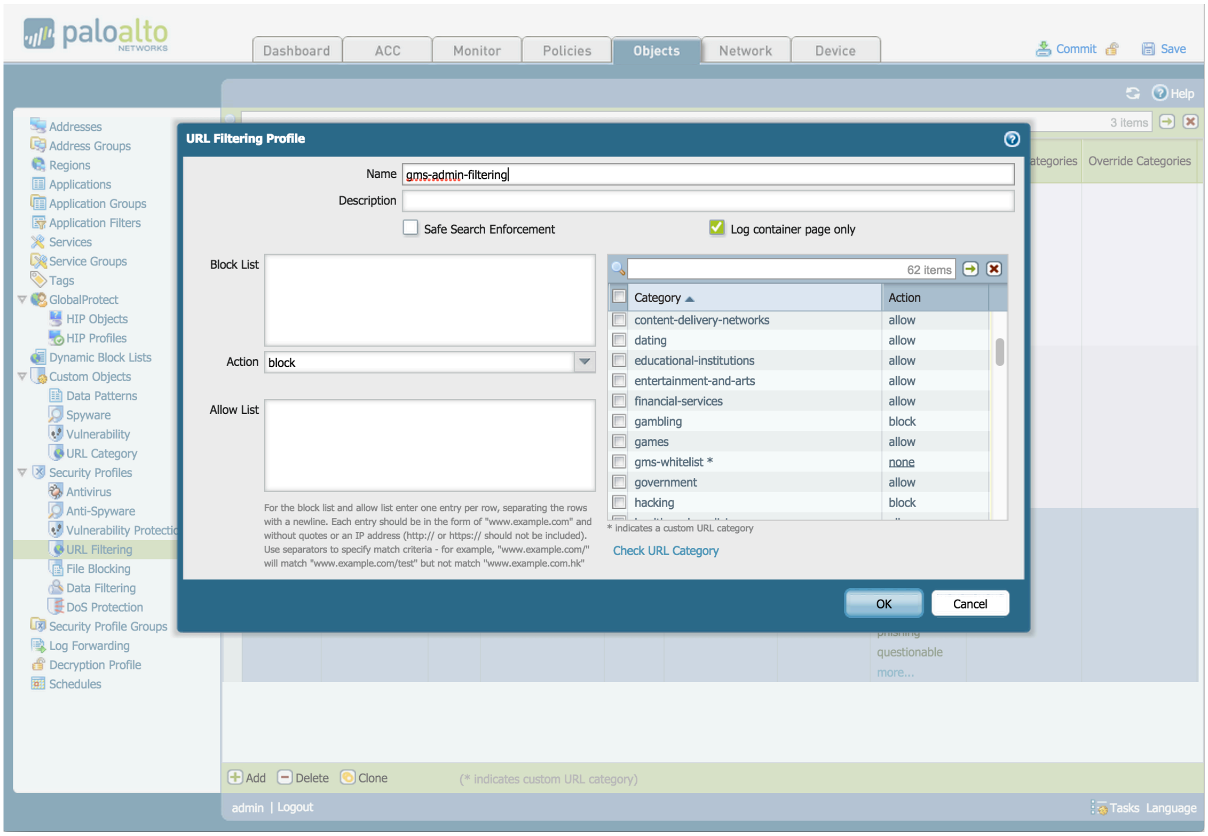
Description:

Sites
□ *.twitter.com
☑ twitter.com

Enter one entry per row.
Each entry may be of the form **www.example.com** or it could have wildcards like **www.*.com**.

Figure 56. Adding the Twitter domains to the list

Next, a URL filtering profile was created for administrators. The “gms-filtering” profile was cloned and renamed to “gms-admin-filtering” (Figure 57).



URL Filtering Profile

Name gms-admin-filtering

Description

□ Safe Search Enforcement ☑ Log container page only

Block List

Action block

Allow List

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

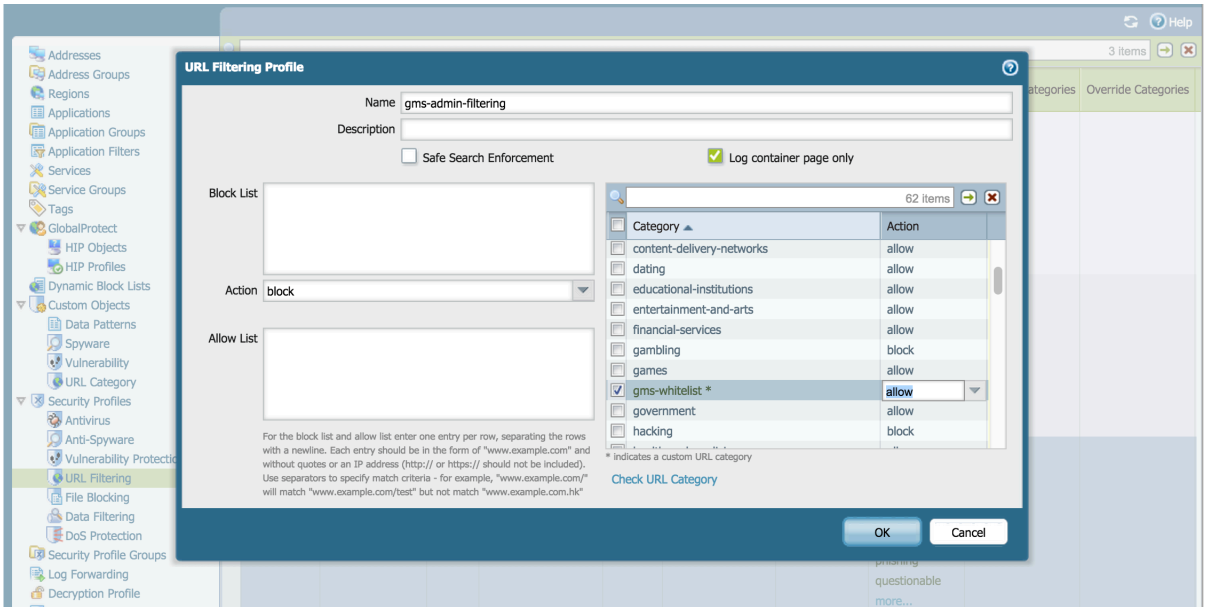
62 items

□	Category ▲	Action
□	content-delivery-networks	allow
□	dating	allow
□	educational-institutions	allow
□	entertainment-and-arts	allow
□	financial-services	allow
□	gambling	block
□	games	allow
□	gms-whitelist *	none
□	government	allow
□	hacking	block

* indicates a custom URL category

Figure 57. Creating a custom URL Filtering profile

The “gms-whitelist” category was set to “allow” (Figure 58) and verified (Figure 59).



URL Filtering Profile

Name gms-admin-filtering

Description

□ Safe Search Enforcement ☑ Log container page only

Block List

Action block

Allow List

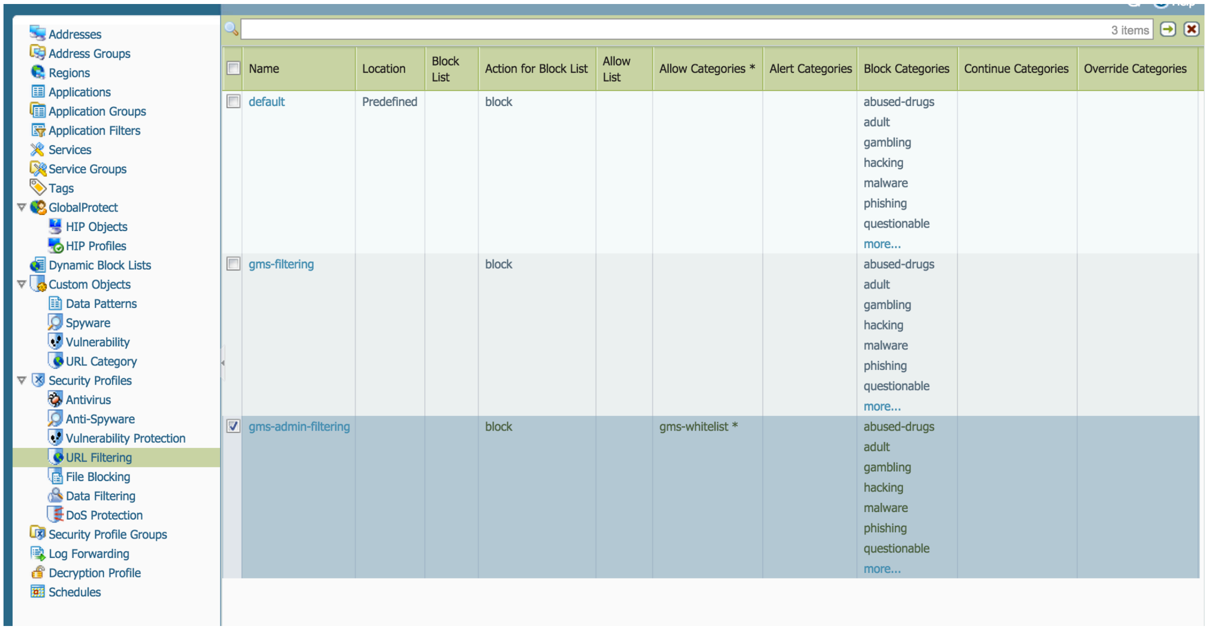
For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

62 items

□	Category ▲	Action
□	content-delivery-networks	allow
□	dating	allow
□	educational-institutions	allow
□	entertainment-and-arts	allow
□	financial-services	allow
□	gambling	block
□	games	allow
☑	gms-whitelist *	allow
□	government	allow
□	hacking	block

* indicates a custom URL category

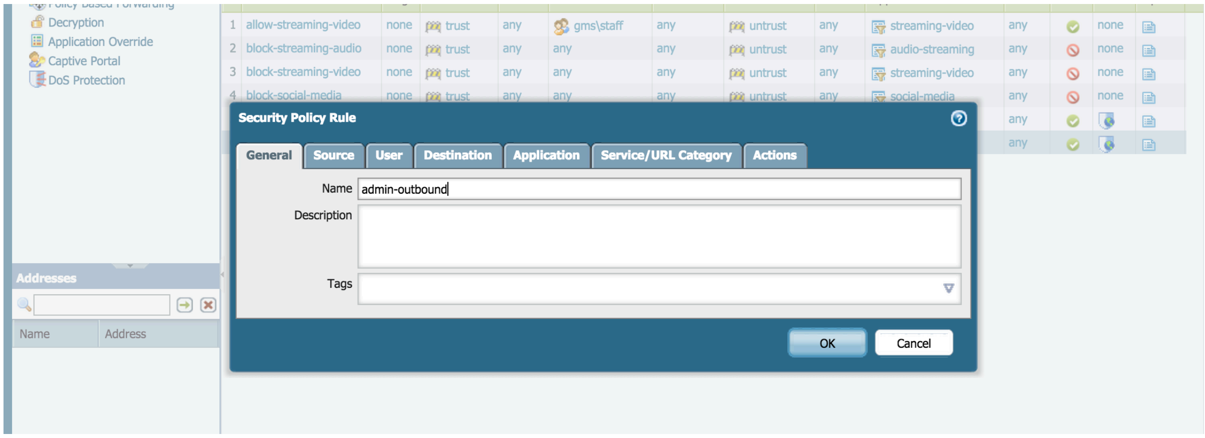
Figure 58. Setting the custom URL category “gms-whitelist” to allow



□	Name	Location	Block List	Action for Block List	Allow List	Allow Categories *	Alert Categories	Block Categories	Continue Categories	Override Categories
□	default	Predefined		block				abused-drugs adult gambling hacking malware phishing questionable more...		
□	gms-filtering			block				abused-drugs adult gambling hacking malware phishing questionable more...		
☑	gms-admin-filtering			block		gms-whitelist *		abused-drugs adult gambling hacking malware phishing questionable more...		

Figure 59. Verifying the URL Filtering profile creation

Next a security rule was created for Principal Jones. The "default-outbound" rule was cloned and renamed "admin-outbound" (Figure 60).



1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	none
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	none
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	none
4	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	none

Security Policy Rule

Name admin-outbound

Description

Tags

Figure 60. Creating the security rule "admin-outbound"

The source user was changed to "gms\bjones" (Figure 61).

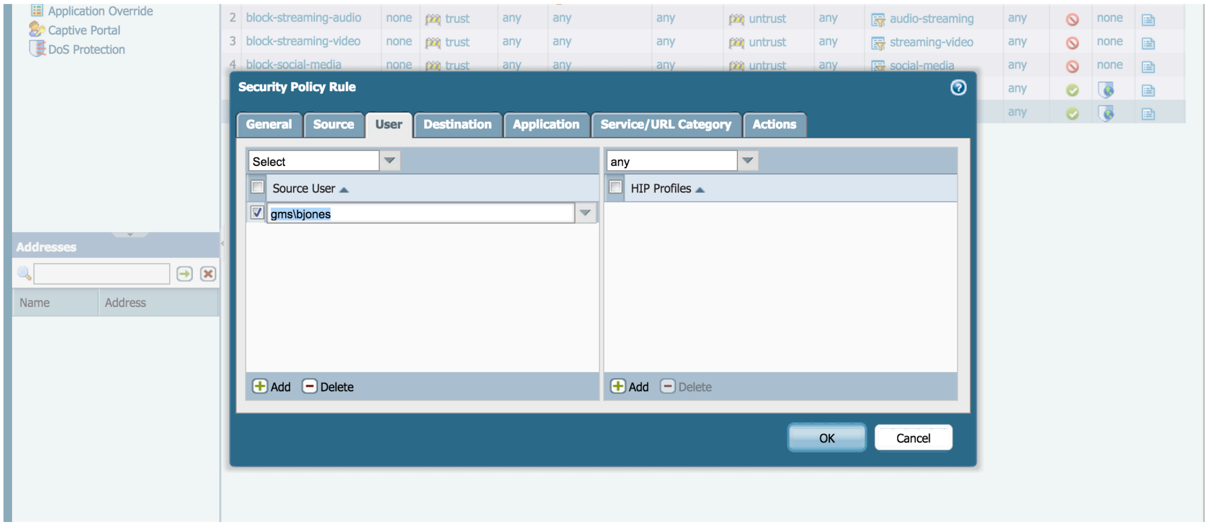

Application Override
Captive Portal
DoS Protection
Addresses
Name
Address
2 block-streaming-audio none trust any any any untrust any audio-streaming any none
3 block-streaming-video none trust any any any untrust any streaming-video any none
4 block-social-media none trust any any any untrust any social-media any none
Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Select
Source User
gms\bjones
any
HIP Profiles
Add
Delete
OK
Cancel

Figure 61. Setting the source user to “gms\bjones”

The “twitter” application was added to the Application tab (Figure 62).

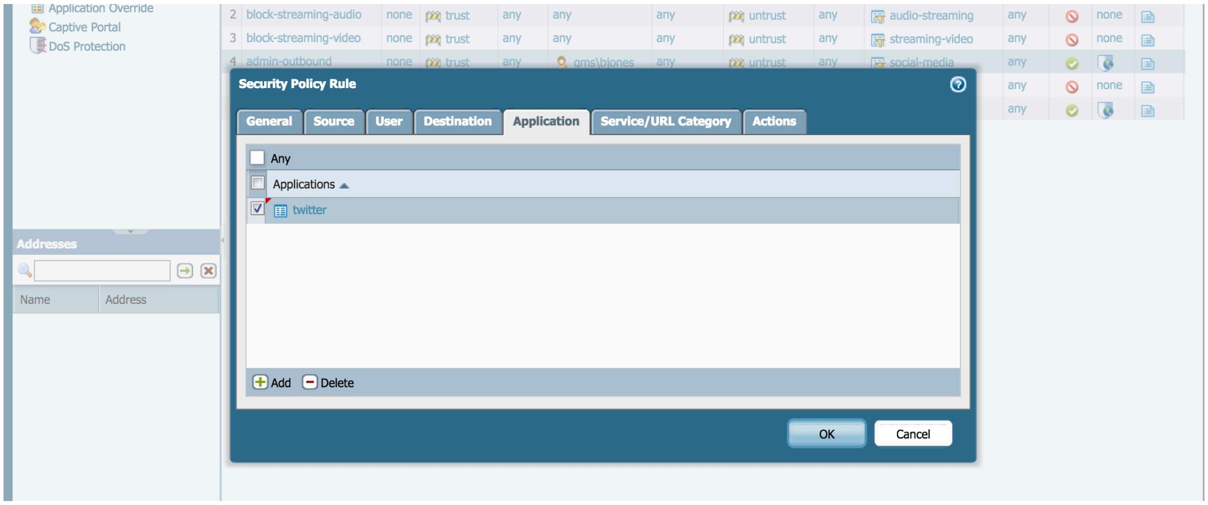
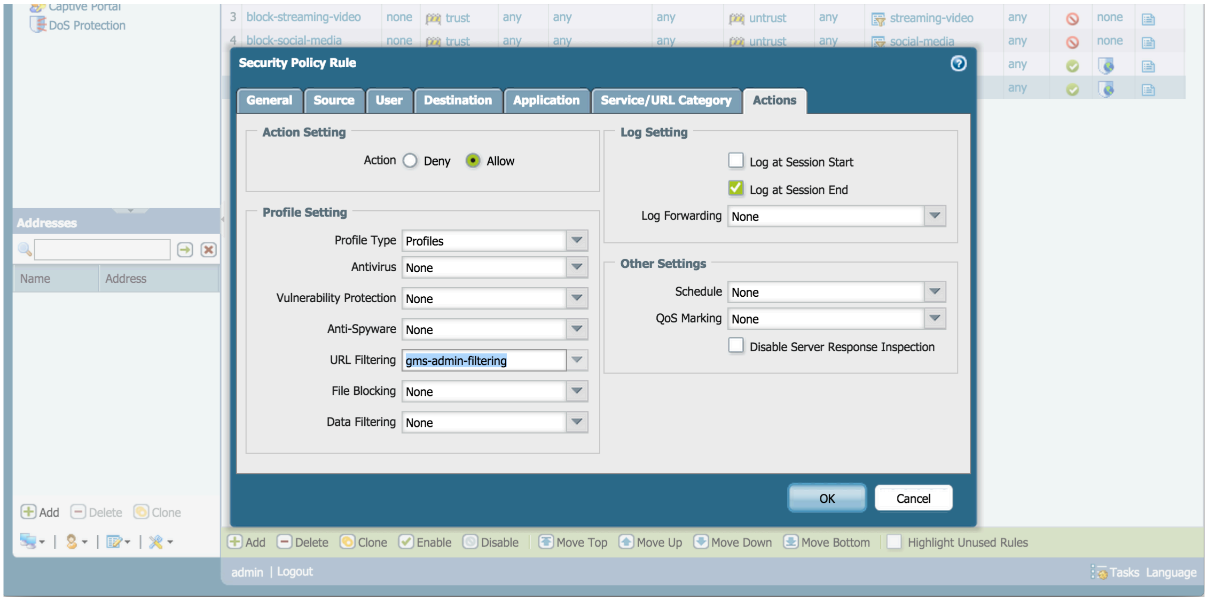

Application Override
Captive Portal
DoS Protection
Addresses
Name
Address
2 block-streaming-audio none trust any any any untrust any audio-streaming any none
3 block-streaming-video none trust any any any untrust any streaming-video any none
4 admin-outbound none trust any gms\bjones any untrust any social-media any
Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Any
Applications
twitter
Add
Delete
OK
Cancel

Figure 62. Adding “twitter” to the Application tab

Under Actions > Profiles > Profile Type > URL Filtering, the option was changed to “gms-admin-filtering” (Figure 63).



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Action Setting

Action ○ Deny ● Allow

Profile Setting

Profile Type: Profiles
Antivirus: None
Vulnerability Protection: None
Anti-Spyware: None
URL Filtering: gms-admin-filtering
File Blocking: None
Data Filtering: None

Log Setting

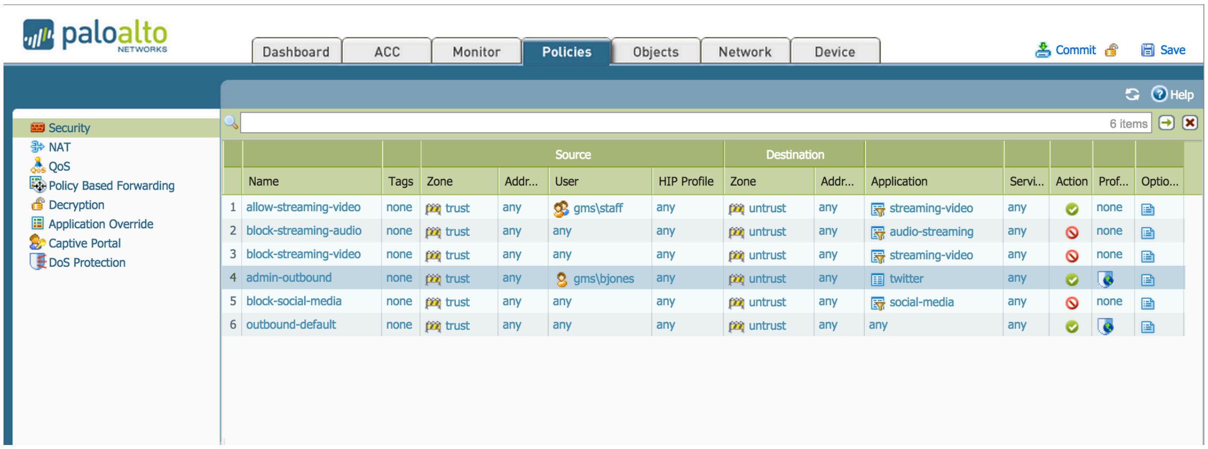
□ Log at Session Start
☑ Log at Session End
Log Forwarding: None

Other Settings

Schedule: None
QoS Marking: None
□ Disable Server Response Inspection

Figure 63. Setting the URL filtering profile

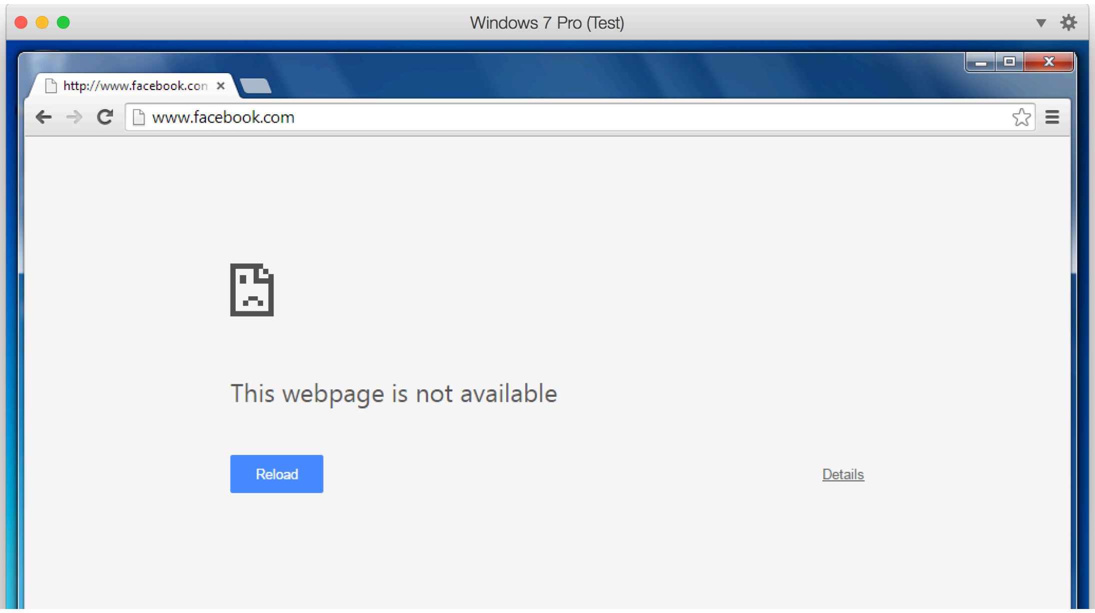
The rule was added, moved above the "block-social-media" rule and verified in the list (Figure 64). It was important the rule was placed properly. If the rule was placed below the "block-social-media", Principal Jones would not be able to access Twitter.



			Source				Destination						
	Name	Tags	Zone	Addr...	User	HIP Profile	Zone	Addr...	Application	Servi...	Action	Prof...	Optio...
1	allow-streaming-video	none	trust	any	gms\staff	any	untrust	any	streaming-video	any	✓	none	▤
2	block-streaming-audio	none	trust	any	any	any	untrust	any	audio-streaming	any	⊘	none	▤
3	block-streaming-video	none	trust	any	any	any	untrust	any	streaming-video	any	⊘	none	▤
4	admin-outbound	none	trust	any	gms\bjones	any	untrust	any	twitter	any	✓	●	▤
5	block-social-media	none	trust	any	any	any	untrust	any	social-media	any	⊘	none	▤
6	outbound-default	none	trust	any	any	any	untrust	any	any	any	✓	●	▤

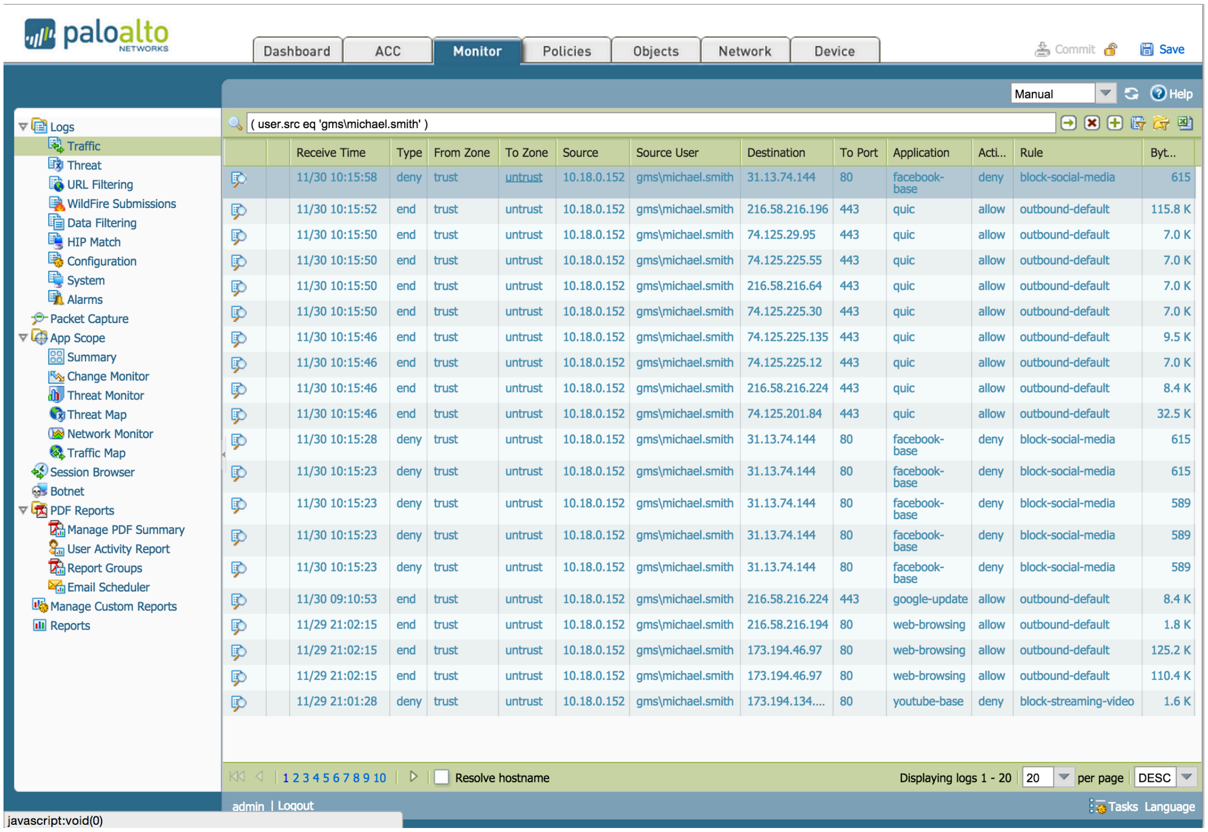
Figure 64. Confirming rule creation and order

The last step was to confirm the rules work as expected. The student user michael.smith attempts to navigate to Facebook but the page failed to load (Figure 65). In Figure 66, the traffic logs are reviewed and the "block-social-media" rule was correctly blocking traffic.



This webpage is not available

Figure 65. Page fails to load for student user account



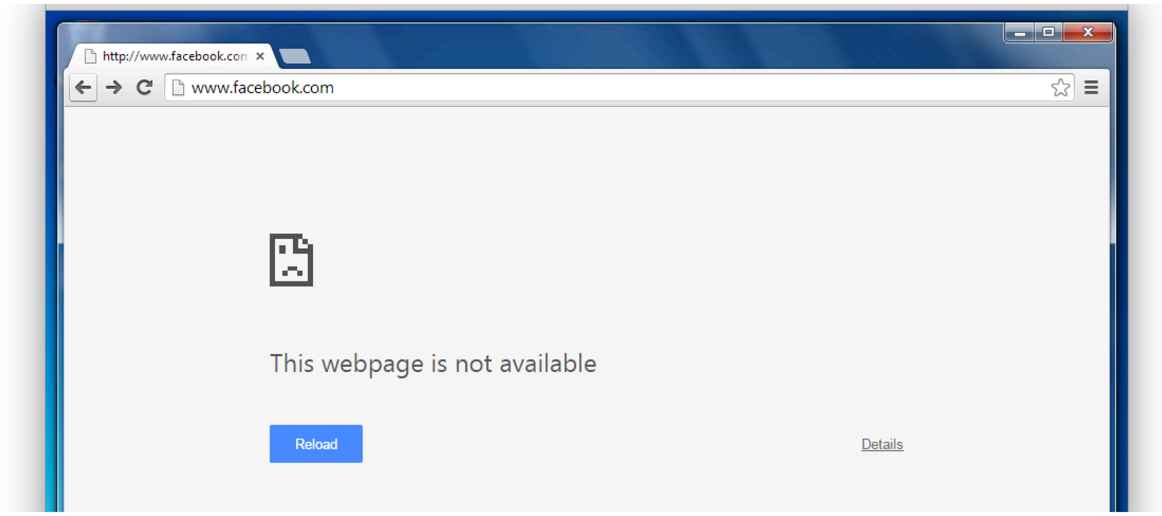
(user.src eq 'gms\michael.smith')

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/30 10:15:58	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:15:52	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.196	443	quic	allow	outbound-default	115.8 K
11/30 10:15:50	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.29.95	443	quic	allow	outbound-default	7.0 K
11/30 10:15:50	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.55	443	quic	allow	outbound-default	7.0 K
11/30 10:15:50	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.64	443	quic	allow	outbound-default	7.0 K
11/30 10:15:50	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.30	443	quic	allow	outbound-default	7.0 K
11/30 10:15:46	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.135	443	quic	allow	outbound-default	9.5 K
11/30 10:15:46	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.225.12	443	quic	allow	outbound-default	7.0 K
11/30 10:15:46	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.224	443	quic	allow	outbound-default	8.4 K
11/30 10:15:46	end	trust	untrust	10.18.0.152	gms\michael.smith	74.125.201.84	443	quic	allow	outbound-default	32.5 K
11/30 10:15:28	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:15:23	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:15:23	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 10:15:23	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 10:15:23	deny	trust	untrust	10.18.0.152	gms\michael.smith	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 09:10:53	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.224	443	google-update	allow	outbound-default	8.4 K
11/29 21:02:15	end	trust	untrust	10.18.0.152	gms\michael.smith	216.58.216.194	80	web-browsing	allow	outbound-default	1.8 K
11/29 21:02:15	end	trust	untrust	10.18.0.152	gms\michael.smith	173.194.46.97	80	web-browsing	allow	outbound-default	125.2 K
11/29 21:02:15	end	trust	untrust	10.18.0.152	gms\michael.smith	173.194.46.97	80	web-browsing	allow	outbound-default	110.4 K
11/29 21:01:28	deny	trust	untrust	10.18.0.152	gms\michael.smith	173.194.134....	80	youtube-base	deny	block-streaming-video	1.6 K

Displaying logs 1 - 20 | 20 per page | DESC

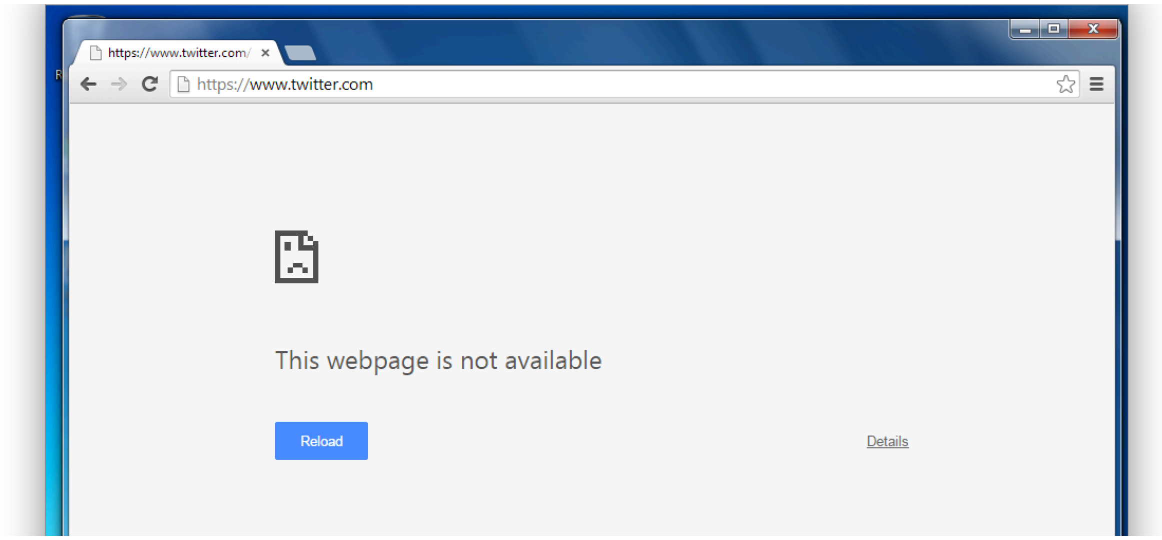
Figure 66. Traffic logs confirm Facebook is blocked

In Figure 67 and Figure 68, the staff user “gbolek” unsuccessfully attempts to navigate to Facebook and Twitter. In Figure 69, the traffic logs show traffic for “gbolek” being blocked per the “block-social-media” rule.



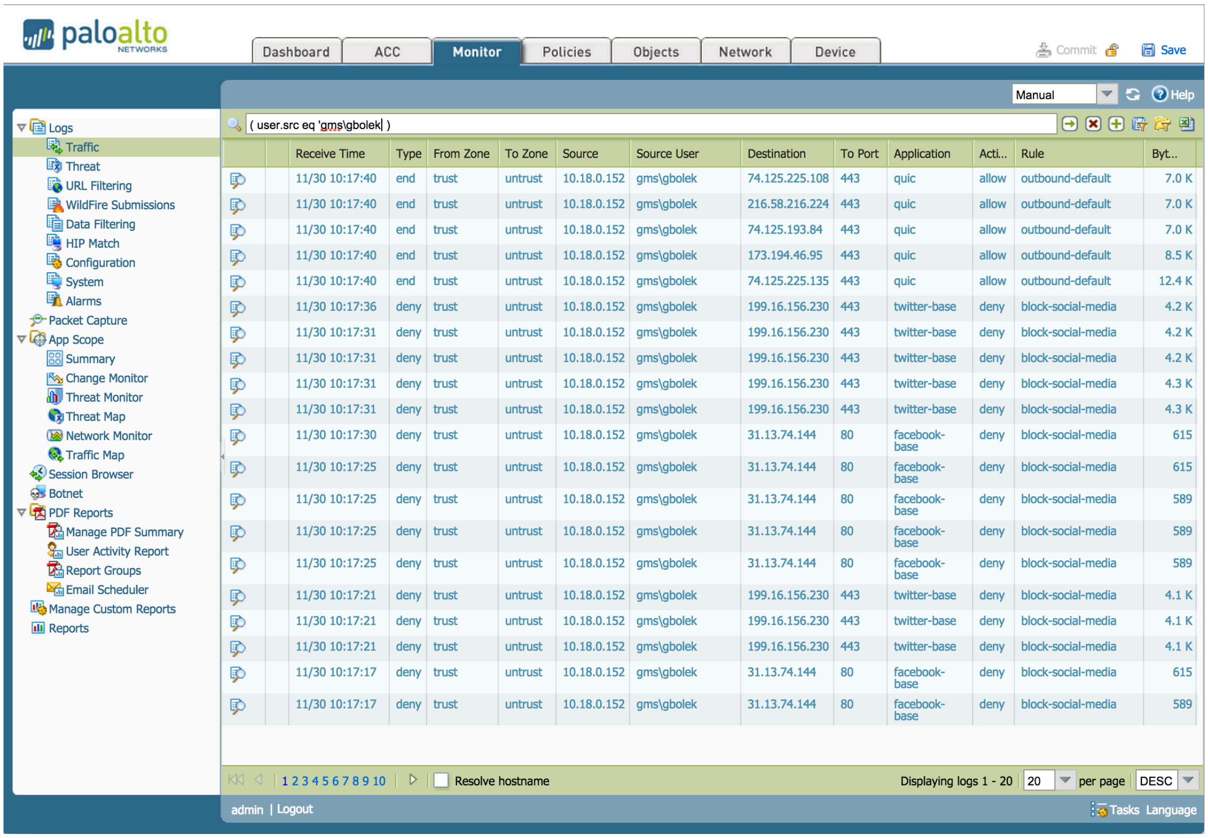
This webpage is not available

Figure 67. Facebook fails to load for staff account



This webpage is not available

Figure 68. Twitter fails to load for staff account



(user.src eq 'gms\gbolek)

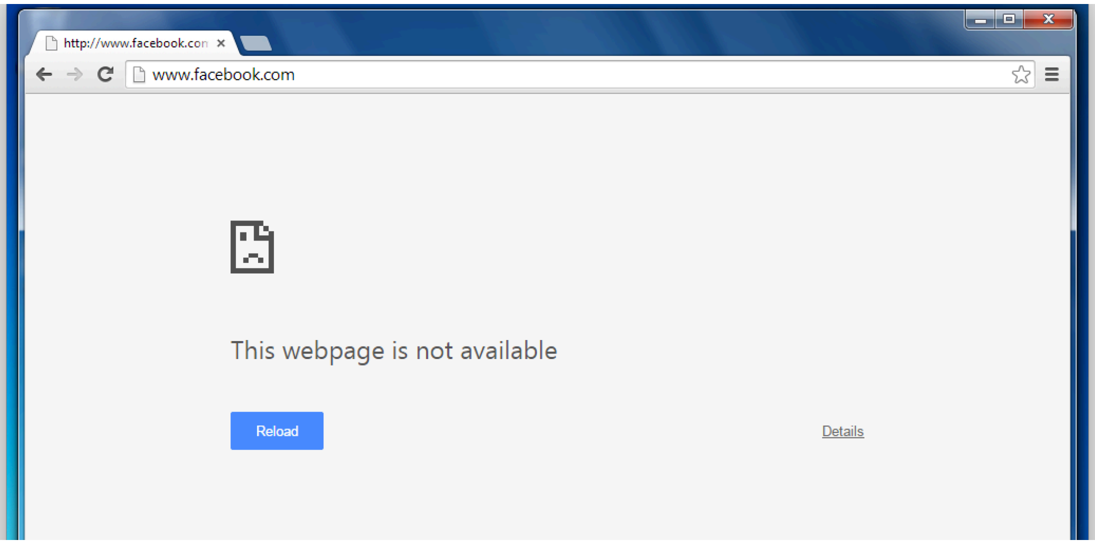
Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/30 10:17:40	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.108	443	quic	allow	outbound-default	7.0 K
11/30 10:17:40	end	trust	untrust	10.18.0.152	gms\gbolek	216.58.216.224	443	quic	allow	outbound-default	7.0 K
11/30 10:17:40	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.193.84	443	quic	allow	outbound-default	7.0 K
11/30 10:17:40	end	trust	untrust	10.18.0.152	gms\gbolek	173.194.46.95	443	quic	allow	outbound-default	8.5 K
11/30 10:17:40	end	trust	untrust	10.18.0.152	gms\gbolek	74.125.225.135	443	quic	allow	outbound-default	12.4 K
11/30 10:17:36	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.2 K
11/30 10:17:31	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.2 K
11/30 10:17:31	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.2 K
11/30 10:17:31	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.3 K
11/30 10:17:31	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.3 K
11/30 10:17:30	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:17:25	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:17:25	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 10:17:25	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 10:17:25	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	589
11/30 10:17:21	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.1 K
11/30 10:17:21	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.1 K
11/30 10:17:21	deny	trust	untrust	10.18.0.152	gms\gbolek	199.16.156.230	443	twitter-base	deny	block-social-media	4.1 K
11/30 10:17:17	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	615
11/30 10:17:17	deny	trust	untrust	10.18.0.152	gms\gbolek	31.13.74.144	80	facebook-base	deny	block-social-media	589

□ Resolve hostname

Displaying logs 1 - 20 | 20 per page | DESC

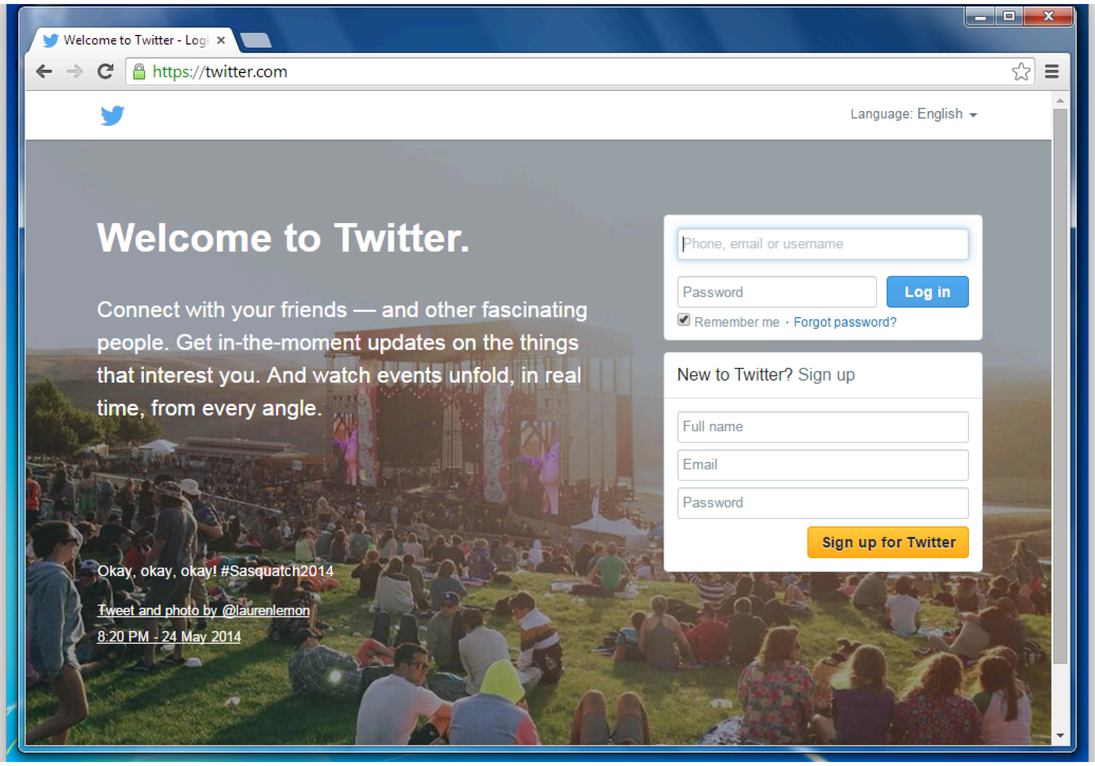
Figure 69. Traffic logs show Facebook and Twitter being blocked

The final test was for Principal Bob Jones staff account. Figure 70, shows user "bjones" unsuccessfully attempting to navigate to Facebook. However, Figure 71, shows Principal Jones was able to load Twitter. In Figure 72, the traffic logs show Facebook traffic being blocked and Twitter traffic being allowed according to their security rules.



This webpage is not available

Figure 70. User is unable to navigate to Facebook



Welcome to Twitter.

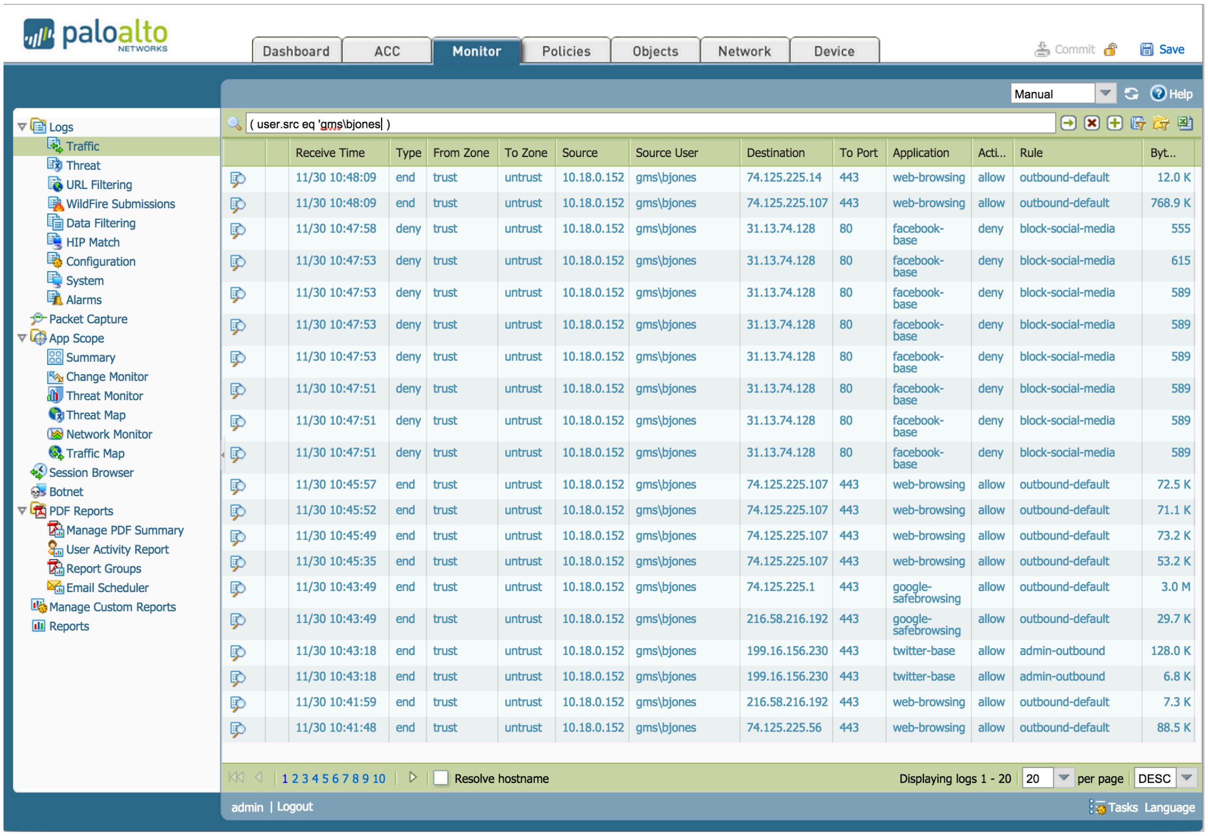
Connect with your friends — and other fascinating people. Get in-the-moment updates on the things that interest you. And watch events unfold, in real time, from every angle.

Okay, okay, okay! #Sasquatch2014

Tweet and photo by @laurenlemon

8:20 PM - 24 May 2014

Figure 71. User successfully loads Twitter



(user.src eq 'gms\bjones)

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Acti...	Rule	Byt...
11/30 10:48:09	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.14	443	web-browsing	allow	outbound-default	12.0 K
11/30 10:48:09	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.107	443	web-browsing	allow	outbound-default	768.9 K
11/30 10:47:58	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	555
11/30 10:47:53	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	615
11/30 10:47:53	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:47:53	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:47:53	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:47:51	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:47:51	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:47:51	deny	trust	untrust	10.18.0.152	gms\bjones	31.13.74.128	80	facebook-base	deny	block-social-media	589
11/30 10:45:57	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.107	443	web-browsing	allow	outbound-default	72.5 K
11/30 10:45:52	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.107	443	web-browsing	allow	outbound-default	71.1 K
11/30 10:45:49	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.107	443	web-browsing	allow	outbound-default	73.2 K
11/30 10:45:35	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.107	443	web-browsing	allow	outbound-default	53.2 K
11/30 10:43:49	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.1	443	google-safebrowsing	allow	outbound-default	3.0 M
11/30 10:43:49	end	trust	untrust	10.18.0.152	gms\bjones	216.58.216.192	443	google-safebrowsing	allow	outbound-default	29.7 K
11/30 10:43:18	end	trust	untrust	10.18.0.152	gms\bjones	199.16.156.230	443	twitter-base	allow	admin-outbound	128.0 K
11/30 10:43:18	end	trust	untrust	10.18.0.152	gms\bjones	199.16.156.230	443	twitter-base	allow	admin-outbound	6.8 K
11/30 10:41:59	end	trust	untrust	10.18.0.152	gms\bjones	216.58.216.192	443	web-browsing	allow	outbound-default	7.3 K
11/30 10:41:48	end	trust	untrust	10.18.0.152	gms\bjones	74.125.225.56	443	web-browsing	allow	outbound-default	88.5 K

☐ Resolve hostname

Displaying logs 1 - 20 | 20 per page | DESC

Figure 72. Traffic logs show Facebook blocked and Twitter allowed

After confirming the behavior and reviewing the Palo Alto traffic logs, all rules were confirmed to be operating correctly. The school IT administrator had successfully blocked streaming audio and video content as well as social media for students. Staff accounts were allowed to stream video. Principal Jones also was given access to Twitter as mandated by the schools new policy. By leveraging the schools existing Active Directory server, the school IT administrator easily created security rules using each of the three core technologies, App-ID, User-ID and Content-ID.

4.6 Summary

By creating a scenario, an example configuration of a Palo Alto firewall was shown for a hypothetical middle school. This scenario illustrates the use of an existing Active Directory server and how rules are configured using Palo Alto's core technologies, App-ID, User-ID and Content-ID. In several figures, screenshots of the Palo Alto traffic logs are provided showing the rules in action. When used together, the Palo Alto core technologies easily allow the creation of complex rule sets to control traffic. In this scenario, the school IT administrator addressed the bandwidth issues the school was having by controlling streaming content (both audio and video) and also reinforced the administration's social media policy.

5. SUMMARY

While school districts continue to look for ways to utilize technology in learning, the technology they utilize continues to change. Teachers and students push school districts to continually rethink their networks and security. The application landscape has evolved to a point where old security tools are no longer adequate. School network administrators need visibility into what applications are running on their networks. Network administrators who do not have Application Layer inspection are not capable of truly securing their network. The solution to this problem is the use of a Next-Generation firewall from Palo Alto.

Palo Alto's NGFW provides technology that is at the cutting edge of security and its benefits to school districts are numerous. The core technologies that Palo Alto has created match perfectly with a school district needs. App-ID allows application identification, User-ID maps traffic to users and Content-ID inspects traffic. When put together they seamlessly integrate, creating a network security platform that is powerful and simplistic. It is easy for school district to block unwanted applications either by individually or by category. Building upon that, security rules can easily be applied to a specific user or group because of the tight integration with a schools directory services. URL filtering is accomplished through categorization, whitelists and blacklists and proves to be extremely flexible.

This paper shows how the 3 core technologies of a Palo Alto Networks NGFW firewall can be used to help secure a K-12 school network. The examples provided are from the experiences of the author and are not exhaustive by any means. Further research could be done to show how encryption affects application identification and how SSL inspection (both outbound and inbound) can be used to solve this issue. Another area of focus could be QoS and how it can be implemented to ensure bandwidth and quality of operation for certain applications or even web sites.

WORKS CITED

[1] The Modern Network. (2014, July) The Modern Network. [Online]. http://themodernnetwork.com/education/next-generation-firewall-protects-schools-cyber-threats/

[2] Barry L. Young. (2008, Aug.) Securing the K-12 School Network through Effective Internet Access Control, Network Traffic Monitoring, and Data Analysis. Document.

[3] Mike Kennedy. (2011, April) American School & University. [Online]. http://asumag.com/Construction/technology/21st-century-learning-201104

[4] Nancye Blair. (2012, Jan/Feb) NAESP. [Online]. http://www.naesp.org/principal-januaryfebruary-2012-technology/technology-integration-new-21st-century-learner

[5] Education Law Center. (2014, May) Education Law Center. [Online]. http://www.edlawcenter.org/news/archives/secondary-reform/testing-concerns-grow-as-parcc-phase-in-begins.html

[6] Dian Schaffhauser. (2011, June) The Journal. [Online]. http://thejournal.com/articles/2011/06/07/high-stakes-online-testing-coming-soon.aspx?sc_lang=en

[7] Dian Schaffhauser. (2014, March) The Journal. [Online]. http://thejournal.com/articles/2014/03/27/report-most-schools-delivering-byod-programs-training-teachers-in-mobile-devices-usage.aspx

[8] Joshua Bolkan. (2013, May) The Journal. [Online]. http://thejournal.com/articles/2013/05/21/report-85-percent-of-educational-institutions-allow-byod-yet-security-lags-behind.aspx

[9] Frank Ohlhorst. (2013, March) Network Computing. [Online]. http://www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097?

[10] Mindi McDowell and Allen Householder. (2013, June) US-CERT. [Online]. https://www.us-cert.gov/ncas/tips/ST04-004

[11] David Cartwright. (2004, Jan.) Computerworld. [Online]. http://www.computerworld.com/article/2574656/security0/stateful-vs--deep-inspection-firewalls.html

[12] CCNA Study Guide. (2010, June) CCNA Study Guide. [Online]. http://ccna5.com/tag/osi-model/

[13] Karen Scarfone and Paul Hoffman. (2009, Sep.) Guidelines on Firewalls and Firewall Policy.

[14] Rik Ferguson. (2012, July) ComputerWeekly. [Online]. http://www.computerweekly.com/news/2240159432/The-history-of-the-Next-Generation-Firewall

[15] Paul Tero. (2013, Jan.) Smashing Magazine. [Online]. http://www.smashingmagazine.com/2013/01/30/introduction-to-firewalls/

[16] Tom Sheldon. (2013, Jan.) Windows Security. [Online]. http://www.windowsecurity.com/whitepapers/windows_security/General_Firewall_White_Paper.html

[17] Margaret Rouse. (2007, Nov.) TechTarget. [Online]. http://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI

[18] Starnet Data Design, Inc. (2013, February) Starnet Data Design, Inc. [Online]. http://www.starnetdata.com/wp-content/uploads/2014/06/2014-Magic-Quadrant-Next-Generation-Firewalls.pdf

[19] Ashley Wainwright. (2013, October) Secure Edge Networks. [Online]. http://www.securedgenetworks.com/secure-edge-networks-blog/bid/95605/Why-Every-School-Wireless-Network-Needs-A-Palo-Alto-Firewall

[20] Palo Alto Networks, Inc. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/company/company-fast-facts.html

[21] Palo Alto Networks, Inc. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/company.html

[22] Palo Alto Networks, Inc. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/products/technologies/app-id.html

[23] Palo Alto Networks, Inc. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/products/technologies/user-id.html

[24] Palo Alto Networks, Inc. Palo Alto Networks. [Online]. https://www.paloaltonetworks.com/products/technologies/content-id.html

[25] Julie Long. (2014, January) Secure Edge Networks. [Online]. http://www.securedgenetworks.com/secure-edge-networks-blog/bid/101766/How-to-Increase-Schools-Bandwidth-with-a-Palo-Alto-Firewall

[26] Sandvine. (2013, Nov.) Sandvine. [Online]. https://www.sandvine.com/pr/2013/11/11/sandvine-report-netflix-and-youtube-account-for-50-of-all-north-american-fixed-network-data.html

[27] Drew Fitzgerald. (2014, May) The Wall Street Journal. [Online].

http://online.wsj.com/articles/SB10001424052702304908304579561802483718502