



4. Screenshot of pfSense NAT forwarding rules required for ns1 and www splunk-forwarding
- a. Remember, only these two boxes should be allowed to communicate with the Splunk server

<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	200.35.23.200	*	200.35.23.208	9997	192.168.1.208	9997	Forwarding to Splunk for ns1 server		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	200.35.23.202	*	200.35.23.208	9997	192.168.1.208	9997	Forwarding to Splunk for www server		

#### 5. Screenshot and answers to suspicious activity question

>	11/10/20 12:45:17.000 AM	Nov 10 06:45:17 mail dovecot: pop3-login: Disconnected (no auth attempts in 10 secs): user=<>, rip=37.56.23.100, lip=192.168.1.204, TLS handshaking: Connection closed, session=<WTmaBbuzOK8l0Bdk> host = mail   source = /var/log/mail.log   sourcetype = syslog
>	11/10/20 12:40:05.000 AM	Nov 10 06:40:05 mail postfix/anvil[267440]: statistics: max cache size 1 at Nov 10 06:36:45 host = mail   source = /var/log/mail.log   sourcetype = syslog
>	11/10/20 12:40:05.000 AM	Nov 10 06:40:05 mail postfix/anvil[267440]: statistics: max connection count 1 for (submission:37.56.23.100) at Nov 10 06:36:45 host = mail   source = /var/log/mail.log   sourcetype = syslog
>	11/10/20 12:40:05.000 AM	Nov 10 06:40:05 mail postfix/anvil[267440]: statistics: max connection rate 1/60s for (submission:37.56.23.100) at Nov 10 06:36:45 host = mail   source = /var/log/mail.log   sourcetype = syslog
>	11/10/20 12:39:34.000 AM	Nov 10 06:39:34 mail dovecot: imap-login: Aborted login (no auth attempts in 0 secs): user=<>, rip=37.56.23.100, lip=192.168.1.204, TLS, session=<XqIq8bqzZMl0Bdk> host = mail   source = /var/log/mail.log   sourcetype = syslog
>	11/10/20 12:36:45.000 AM	Nov 10 06:36:45 mail postfix/submission/smtpd[267438]: disconnect from unknown[37.56.23.100] ehlo=2 starttls=1 quit=1 commands=4 host = mail   source = /var/log/mail.log   sourcetype = syslog

- a. What is going on?  
On my mail server, there seems to be numerous connection/login attempts through imap, smtp, and pop3.
- b. Is this dangerous?  
Potentially, I think the attacker is probably attempting to brute force their way onto the mail server, so gaining control of this server gives them a gateway onto the private network behind the DMZ. It would be dangerous for them to be able to freely access services on this network like the ldap and www2 server.
- c. Where is it originating?  
It seems to be coming from the IP 37.56.23.100
- d. How might you prevent this, if you were so inclined?  
One idea could be to block connections from that IP address in pfsense, but then they can just use/spoof a different IP.

6. Screenshot and observations of "ET SCAN" or "ET POLICY" entry  
(Looking at the very first entry going to Morocco)

446 3 63 06:54:41 ET SCAN Potential SSH Scan 2001219 6 8.503%

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 22 (msg:"ET SCAN Potential SSH Scan"; flags:S,12; threshold: type both, track by\_src, count 5, seconds 120; reference:url [en.wikipedia.org/wiki/Brute\\_force\\_attack](https://en.wikipedia.org/wiki/Brute_force_attack); reference:url [doc.emergingthreats.net/2001219](https://doc.emergingthreats.net/2001219); classtype:attempted-recon; sid:2001219; rev:19; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;)

file: downloaded.rules:12048

☒ CATEGORIZE 446 EVENT(S) CREATE FILTER: [src](#) [dst](#) [both](#)

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
11		2020-11-10 06:54:41	37.56.23.100	102	SAUDI ARABIA (.sa)	105.148.172.206	5	MOROCCO (.ma)
32		2020-11-10 06:53:47	37.56.23.100	102	SAUDI ARABIA (.sa)	100.48.141.206	11	UNITED STATES (.us)
35		2020-11-10 06:53:31	37.56.23.100	102	SAUDI ARABIA (.sa)	57.45.85.206	9	BELGIUM (.be)
33		2020-11-10 06:52:42	37.56.23.100	102	SAUDI ARABIA (.sa)	72.208.195.206	7	UNITED STATES (.us)
18		2020-11-10 06:50:27	37.56.23.100	102	SAUDI ARABIA (.sa)	151.82.135.206	6	ITALY (.it)
42		2020-11-10 06:50:26	37.56.23.100	102	SAUDI ARABIA (.sa)	183.153.190.206	8	CHINA (.cn)
20		2020-11-10 06:48:07	37.56.23.100	102	SAUDI ARABIA (.sa)	214.130.170.206	8	UNITED STATES (.us)

- When did the event take place?  
2020-11-10 at 6:54:41
- Which IP initiated the traffic?  
The 37.56.23.100 IP
- Where was the traffic directed at?  
It is directing traffic at the 105.148.172.206 device
- What service was involved? (ssh, ftp, smtp, etc.)  
The traffic is scanning SSH

7.

8. Screenshots and details of *three* hosts being attacked
  - a. Pick and report on three hosts these scans are being directed at.  
(I just took shots of all my servers that I could find in the squert)



### My NS1 server:

162	186	1	1		07:01:45	ET SCAN Suspicious inbound to MSSQL port 1433	2010935	6	21.986%
alert tcp \$EXTERNAL_NET any -> \$HOME_NET 1433 (msg:"ET SCAN Suspicious inbound to MSSQL port 1433"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; metadata: former_category POLICY; reference:url, <a href="http://doc.emergingthreats.net/2010935">doc.emergingthreats.net/2010935</a> ; classtype:bad-unknown; sid:2010935; rev:3; metadata:created_at 2010_07_30, updated_at 2018_03_27;)									
file: <b>downloaded.rules:12178</b>									
<input checked="" type="checkbox"/> CATEGORIZE 162 EVENT(S) <input type="checkbox"/> CREATE FILTER: <a href="#">src</a> <a href="#">dst</a> <a href="#">both</a>									
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
162		2020-11-10 07:01:45	37.56.23.50	7	SAUDI ARABIA (.sa)	200.35.23.200	7	VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	
218	284	1	1		07:01:40	ET SCAN Suspicious inbound to mySQL port 3306	2010937	6	27.022%
alert tcp \$EXTERNAL_NET any -> \$HOME_NET 3306 (msg:"ET SCAN Suspicious inbound to mySQL port 3306"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; metadata: former_category POLICY; reference:url, <a href="http://doc.emergingthreats.net/2010937">doc.emergingthreats.net/2010937</a> ; classtype:bad-unknown; sid:2010937; rev:3; metadata:created_at 2010_07_30, updated_at 2018_03_27;)									
file: <b>downloaded.rules:12180</b>									
<input checked="" type="checkbox"/> CATEGORIZE 218 EVENT(S) <input type="checkbox"/> CREATE FILTER: <a href="#">src</a> <a href="#">dst</a> <a href="#">both</a>									
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
218		2020-11-10 07:01:40	37.56.23.50	7	SAUDI ARABIA (.sa)	200.35.23.200	7	VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	

### My www Server:

53	80	1	1		07:31:00	ET SCAN Potential SSH Scan OUTBOUND	2003068	6	3.416%
alert tcp \$HOME_NET any -> \$EXTERNAL_NET 22 (msg:"ET SCAN Potential SSH Scan OUTBOUND"; flags:S,12; threshold: type threshold, track by_src, count 5, seconds 120; reference:url, <a href="http://en.wikipedia.org/wiki/Brute_force_attack">en.wikipedia.org/wiki/Brute_force_attack</a> ; reference:url, <a href="http://doc.emergingthreats.net/2003068">doc.emergingthreats.net/2003068</a> ; classtype:attempted-recon; sid:2003068; rev:6; metadata:created_at 2010_07_30, updated_at 2010_07_30;)									
file: <b>downloaded.rules:12070</b>									
<input checked="" type="checkbox"/> CATEGORIZE 53 EVENT(S) <input type="checkbox"/> CREATE FILTER: <a href="#">src</a> <a href="#">dst</a> <a href="#">both</a>									
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
53		2020-11-09 07:31:00	163.88.94.199	7	FRANCE (.fr)	200.35.23.202	7	VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	
355	492	2	1		07:01:40	ET SCAN Suspicious inbound to mySQL port 3306	2010937	6	21.008%
alert tcp \$EXTERNAL_NET any -> \$HOME_NET 3306 (msg:"ET SCAN Suspicious inbound to mySQL port 3306"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track by_src; metadata: former_category POLICY; reference:url, <a href="http://doc.emergingthreats.net/2010937">doc.emergingthreats.net/2010937</a> ; classtype:bad-unknown; sid:2010937; rev:3; metadata:created_at 2010_07_30, updated_at 2018_03_27;)									
file: <b>downloaded.rules:12180</b>									
<input checked="" type="checkbox"/> CATEGORIZE 355 EVENT(S) <input type="checkbox"/> CREATE FILTER: <a href="#">src</a> <a href="#">dst</a> <a href="#">both</a>									
QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
218		2020-11-10 07:01:40	37.56.23.50	7	SAUDI ARABIA (.sa)	200.35.23.202	7	VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	
137		2020-11-10 06:30:57	163.88.94.199	7	FRANCE (.fr)	200.35.23.202	7	VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	

### My Mail Server:

0	22	2	1	 	00:08:27	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack			2002995	6	100.000%
alert tcp \$EXTERNAL_NET any -> \$HOME_NET 993 (msg:"ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack"; flags: S,12; threshold: type both, track by_src, count 30, seconds 60; reference:url <a href="http://doc.emergingthreats.net/2002995">doc.emergingthreats.net/2002995</a> ; classtype:misc-activity; sid:2002995; rev:9; metadata:created_at 2010_07_30, updated_at 2010_07_30;)											
file: <b>downloaded.rules:12069</b>											
<input checked="" type="checkbox"/> CATEGORIZE 22 EVENT(S)  CREATE FILTER: <a href="#">src</a> <a href="#">dst</a> <a href="#">both</a>											
QUEUE	TOTAL	CLASS	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY	
0	1			2020-11-04 00:08:27	 37.56.23.100	102	 SAUDI ARABIA (.sa)	 200.35.23.204	7	 VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	
0	21			2020-11-03 17:17:55	 37.56.23.50	7	 SAUDI ARABIA (.sa)	 200.35.23.204	7	 VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)	


### My www2 server:

0

111

1

1



00:03:36

ET SCAN Potential SSH Scan


2001219

6






100.000%

alert tcp \$EXTERNAL\_NET any -> \$HOME\_NET 22 (msg:"ET SCAN Potential SSH Scan"; flags:S,12; threshold: type both, track by\_src, count 5, seconds 120; reference:url [en.wikipedia.org/wiki/Brute\\_force\\_attack](http://en.wikipedia.org/wiki/Brute_force_attack); reference:url [doc.emergingthreats.net/2001219](http://doc.emergingthreats.net/2001219); classtype:attempted-recon; sid:2001219; rev:19; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;)

file: downloaded.rules:12048

☒ CATEGORIZE 111 EVENT(S) 

CREATE FILTER: [src](#) [dst](#) [both](#)

QUEUE	TOTAL	CLASS	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
0	111	 		2020-11-04 00:03:36	 37.56.23.100	102	 SAUDI ARABIA (.sa)	 200.35.23.206	7	 VENEZUELA, BOLIVARIAN REPUBLIC OF (.ve)

#### b. Who is initiating these attacks?

There are three IPs coming from either Saudi Arabia or France that are attacking my servers. These are 37.56.23.50 and 37.56.23.100 from Saudi Arabia and 162.88.94.199 from France. They seem to be scanning for MSSQL, MySQL, SSH, and IMAP services running on the machines.