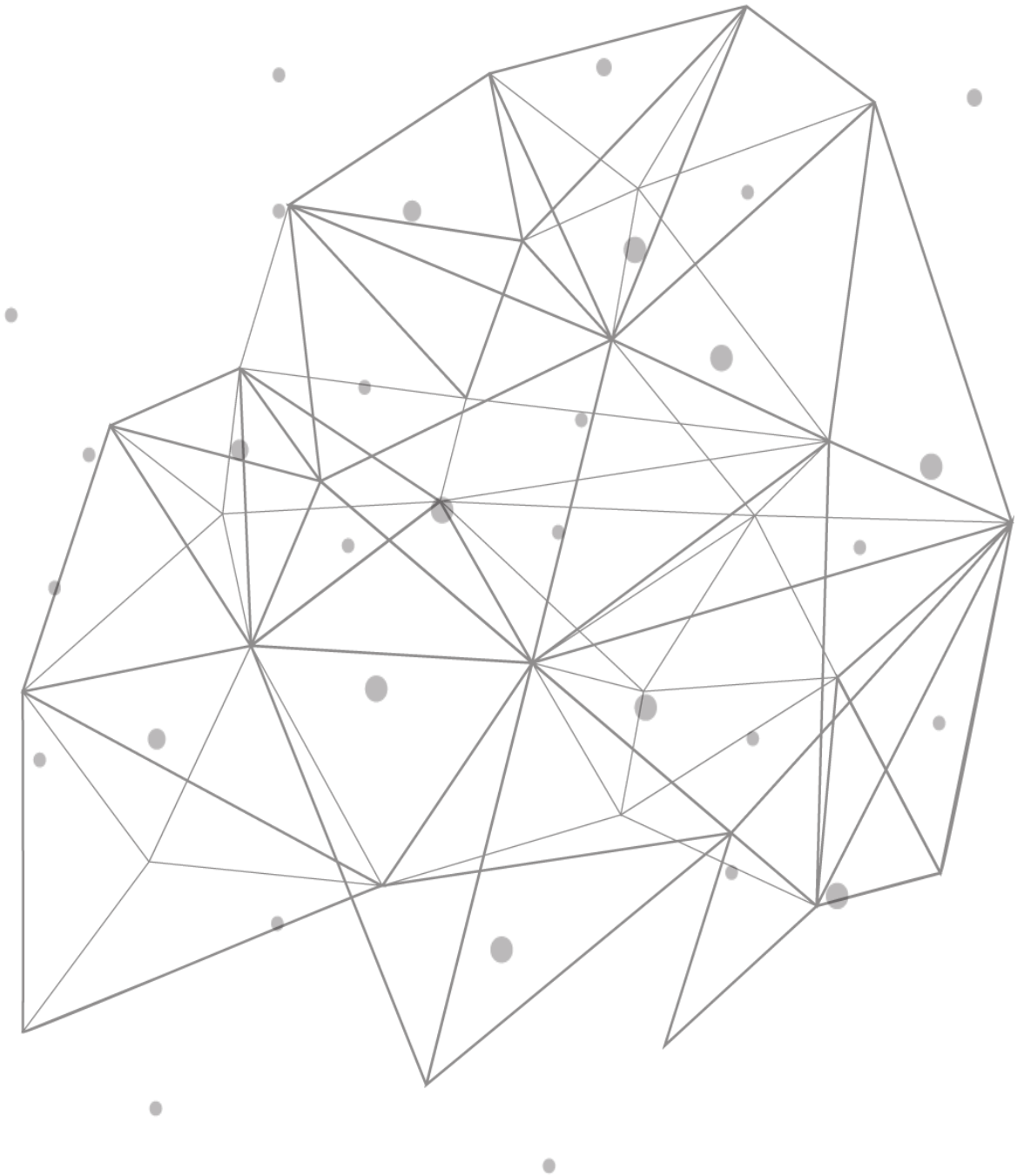
TCPWave DDI – DNS Blackhole ACL



Introduction

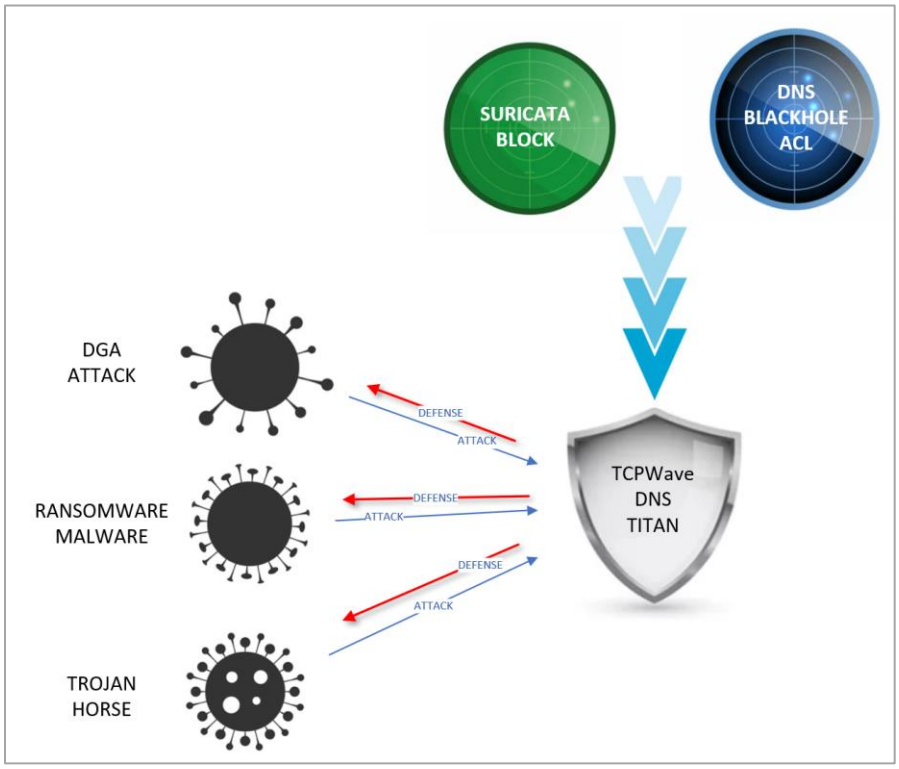
DNS security is one of the critical components of network security infrastructure that is an everlasting field of turmoil and sweating. Defense mechanisms are shattered, and counterattacks are planned frequently. Hence the networks tend to be vulnerable due to the malicious traffic. It requires a nip in the bud mechanism. One such option to restrict the malicious traffic flow is the usage of Access Control Lists (ACLs). This whitepaper provides insights on auto-blocking malicious traffic using DNS Blackhole ACL mechanism in the TCPWave IPAM application.

About DNS Blackhole ACL

The DNS Blackhole ACL feature provides the ability to specify the IP address of a client that you do not want to use in the DNS resolution process. The ACL is auto-created when the anomaly detection alerts the TCPWave IPAM application. The recursive cache blocks the source IP at layer 7 or the application layer. On the other hand, Suricata filters at layer 4 or transport Layer.

DNS Blackhole ACL Mechanism in TCPWave IPAM

In the TCPWave IPAM application, if a source IP is declared as malicious by our Network Security Monitoring (NSM) platform, then it is added to blackhole option section of the DNS appliance configuration. The architecture is shown as below:

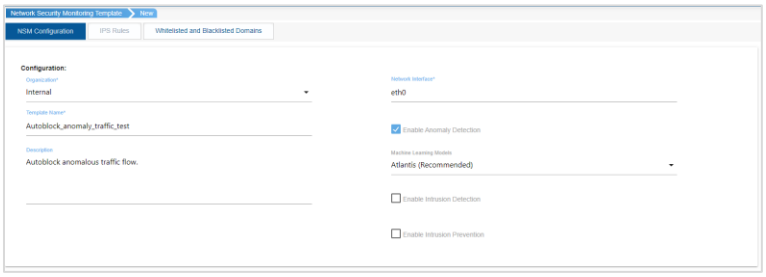


The process to automatically block anomalous traffic by using DNS Blackhole ACL option is as follows:

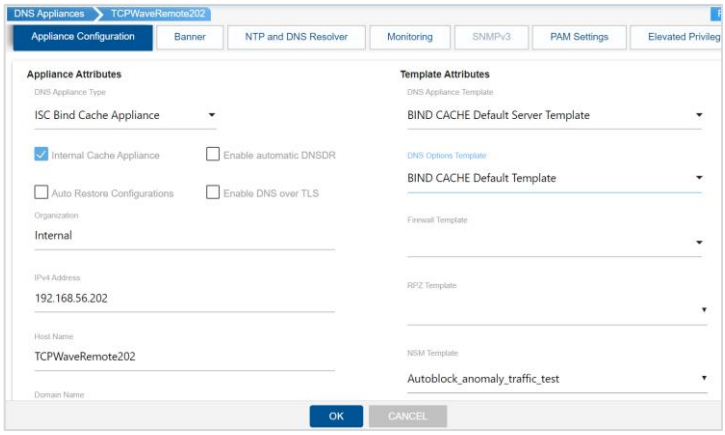
Anomaly Detection

To initiate the anomaly detection process on the DNS remote appliance:

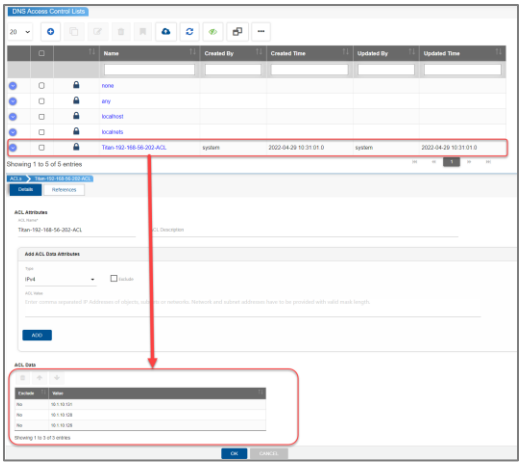
- Create NSM template with Anomaly Detection enabled on it.



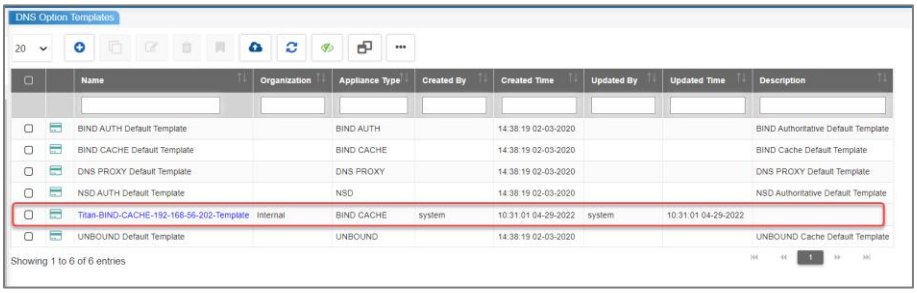
- Associate the created NSM template to the DNS remote appliance.



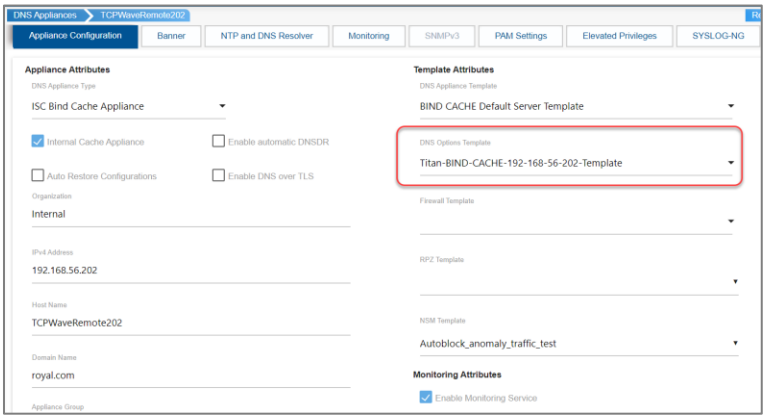
- Navigate to Administration >> Configuration Management >> Global Policy Management, complete the following:
    - Set the global option **Automatically block anomalous traffic on DNS Caches** to Yes. By default, this feature is disabled to No.
    - Set the global option **Anomalous Traffic Blocking Methodologies** to Blackhole ACL.
- The list of malicious source IP address are generated based on the Machine Learning techniques. RemoteMonitStatsoperation scheduled job executes for every five minutes and the standard ACLs with the anomalous source IP address are auto created in the DNS Access Control Lists >> ACL data grid of the IPAM.
- The naming convention to create ACL: Titan- <DNS appliance IP> -ACL



- The system auto-creates a DNS Option Template with the blackhole ACLs.



- The auto-created DNS Option Template which has the blackhole ACLs is associated with the DNS appliance that is under the anomalous traffic.



- As the associated template has blackhole ACL defined in it, the blackhole option section in named.conf file on the DNS appliance is updated.

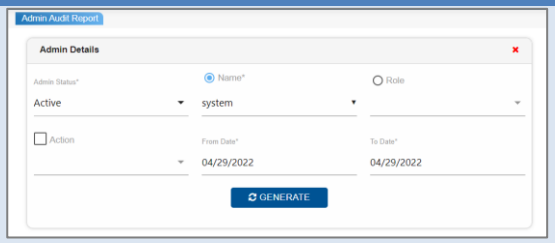
```
#------------------------
# ACLs
#------------------------
acl "Titan-192-168-56-202-ACL" {
        10.1.10.131;10.1.10.128;10.1.10.126;
};
```

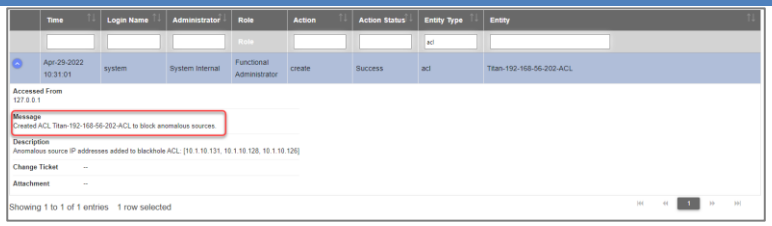
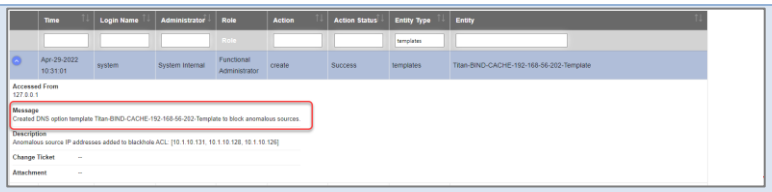
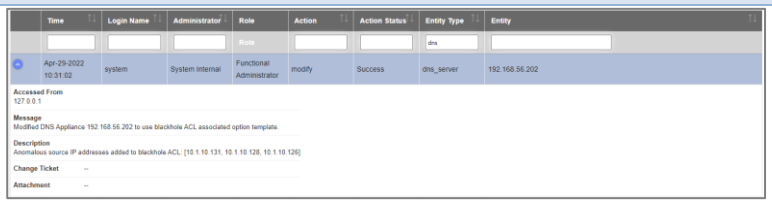
```
#-------------------------
# Global Options
#-------------------------
options {
        response-policy {
        } qname-wait-recurse yes;
        directory "/";
        allow-query {any;};
        allow-transfer {none;};
        blackhole {Titan-192-168-56-202-ACL;};
        dnssec-validation yes;
        listen-on-v6 {none;};
```

- Post the changes in the named.conf, the malicious sources reported by anomaly-detection are blocked from communicating the DNS appliances.
- The network administrators can remove these blocked sources from blackhole ACL after the specified time interval in hours using the global option **DNS Network Security Monitoring Autoblock Purge Interval**.

Audit Management

The audit management help the organizations to gain visibility, identify the security risks by uncovering the underlying network issues, thereby improving the overall network architecture. The operations of ACL, DNS Option Template and DNS appliance performed internally by system user as part of autoblock anomalous traffic functionality is audited. These operations can be viewed at Reports >> Change Reconciliation >> Adhoc Audit Report as shown:

Description	Screenshot
Adhoc Audit Report	

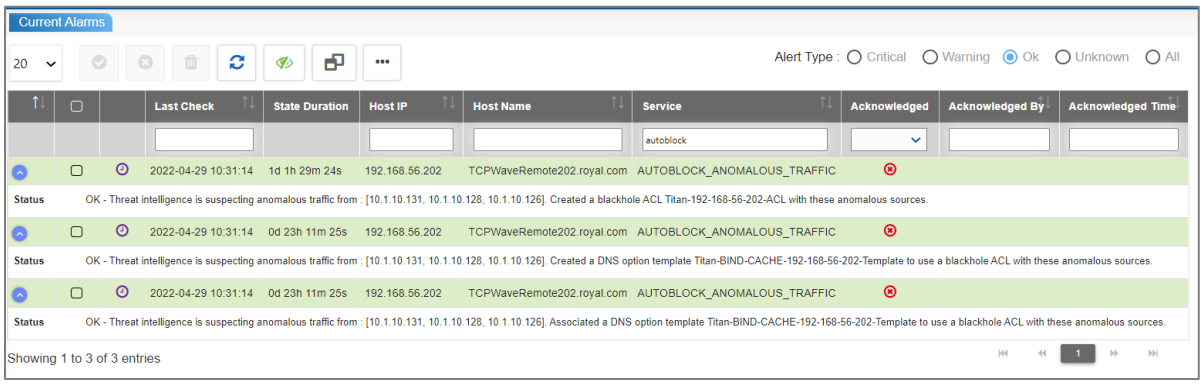
Description	Screenshot
Auto-created ACL	
Auto-created DNS Option Template	
	

Fault Management

With TCPWave's Infrastructure Management, organizations can avail monitoring activities in real-time and fetch predictive analytics to detect the issues.

Alerts

The alerts are generated in Fault Management >> Current Alarms section for all the operations that are performed while configuring ACLs, DNS Option Template, NSM Template, DNS Appliance, as part of autoblock anomalous traffic functionality. The system generates OK alerts when the auto-block operation is successful and generates critical alert when the auto-block operation fails. The network administrators needs to view the logs to take an appropriate action in fixing the issue related to critical alert.



Conclusion

The TCPWave's comprehensive security solutions effectively shield the organizations from the widest range of attacks, uncovers attacker infrastructure there by improving security stack, efficiency, productivity, maintaining service uptime for your organization. For a demo, contact the TCPWave Sales Team