```
{
   "version": "2.0",
   "name": "Scan an asset on DNS FW hit",
   "comment": "Scan an asset on DNS FW hit",
   "type": "REST_EVENT",
   "event_type": [
      "RPZ",
      "TUNNEL"
   ],
   "action_type": "Scan an asset based on DNS FW Hit",
   "content_type": "text/xml",
   "vendor_identifier": "Qualys 2.0",
   "headers": {
      "X-Requested-With": "InfobloxDDIIntegration"
   },
   "quoting": "XML",
   "steps": [
      {
         "name": "Debug#0",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "debugEventsVars",
         "operation": "NOP",
         "body": "${XC:DEBUG:{E:}}"
      },
      {
         "name": "Debug#1",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "assignScanTime",
         "operation": "NOP",
         "body_list": [
            "${XC:COPY:{L:ScanTime}:
{UT:TIME}}${XC:FORMAT:TRUNCATE:{L:ScanTime}:{10t}}"
```

```
      ]
    },
    {
      "name": "checkIPEAs",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${E::ip.extattrs{Qualys_Scan}}",
            "op": "==",
            "right": ""
          },
          {
            "left": "${E::ip.extattrs{Qualys_Scanner}}",
            "op": "==",
            "right": ""
          },
          {
            "left": "${E::ip.extattrs{Qualys_Scan_Option}}",
            "op": "==",
            "right": ""
          }
        ],
        "next": "checkNetEAs"
      }
    },
    {
      "name": "Debug#2",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "setLIPVars",
      "operation": "NOP",
      "body_list": [
        "${XC:COPY:{L:source_ip}:{E:source_ip}}",
        "${XC:COPY:{L:Qualys_Scanner}:
{E:ip.extattrs{Qualys_Scanner}}}",
        "${XC:COPY:{L:Qualys_Scan_Option}:
```

```
{E:ip.extattrs{Qualys_Scan_Option}}}",
        "${XC:COPY:{L:Qualys_Scan}:{E:ip.extattrs{Qualys_Scan}}}",
        "${XC:ASSIGN:{L:EndPointType}:{S:Lease}}"
      ]
    },
    {
      "name": "Debug#3",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "goToDNSFWorAnalytics",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "",
            "op": "==",
            "right": ""
          }
        ],
        "next": "performScanCheck"
      }
    },
    {
      "name": "Debug#4",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "checkNetEAs",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${E::network.extattrs{Qualys_Scan}}",
            "op": "==",
            "right": ""
          },
          {
            "left": "${E::network.extattrs{Qualys_Scanner}}",
            "op": "==",
            "right": ""
          },
          {
            "left": "${E::network.extattrs{Qualys_Scan_Option}}",
            "op": "==",
            "right": ""
          }
        ],
        "stop": true
      }
    },
    {
      "name": "Debug#5",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "setLNetVars",
      "operation": "NOP",
      "body_list": [
        "${XC:COPY:{L:source_ip}:{E:source_ip}}",
        "${XC:COPY:{L:Qualys_Scanner}:
{E:network.extattrs{Qualys_Scanner}}}",
        "${XC:COPY:{L:Qualys_Scan_Option}:
{E:network.extattrs{Qualys_Scan_Option}}}",
        "${XC:COPY:{L:Qualys_Scan}:
{E:network.extattrs{Qualys_Scan}}}",
        "${XC:ASSIGN:{L:EndPointType}:{S:Unknown}}"
      ]
    },
    {
      "name": "Debug#6",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
```

```
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "performScanCheck",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "AND",
        "statements": [
          {
            "left": "${L::Qualys_Scan}",
            "op": "==",
            "right": "false"
          }
        ],
        "stop": true
      }
    },
    {
      "name": "Debug#7",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "DNSFWorAnalytics",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${E::query_name}",
            "op": "==",
            "right": ""
          }
        ],
        "eval": "${XC:ASSIGN:{L:EventType}:{S:DNS Tunneling}}",
        "else_eval": "${XC:ASSIGN:{L:EventType}:{S:DNS Firewall hit}}"
      }
    },
    {
      "name": "Debug#8",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "DNSFWorAnalytics1",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${E::query_name}",
            "op": "!=",
            "right": ""
          }
        ],
        "eval": "${XC:COPY:{L:BlockedDomain}:{E:query_name}",
        "else_eval": "${XC:COPY:{L:BlockedDomain}:
{E:domain_name}}"
      }
    },
    {
      "name": "Debug#9",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "DNSFWorAnalytics2",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${E::query_name}",
            "op": "!=",
            "right": ""
          }
        ],
        "eval": "${XC:COPY:{L:RPZRule}:{E:rule_name}",
        "else_eval": "${XC:ASSIGN:{L:RPZRule}:{S: }}"
      }
    },
    {
      "name": "Debug#10",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "checkIfScanRunning",
      "operation": "POST",
      "transport": {
        "path": "/api/2.0/fo/scan/"
      },
      "parameters": [
        {
          "name": "action",
          "value": "list"
        },
        {
          "name": "target",
          "value": "${E:A:source_ip}"
        },
        {
          "name": "state",
          "value": "Running,Queued"
        }
      ],
      "parse": "XML"
    },
    {
      "name": "Debug#11",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "checkScanRunning",
         "operation": "CONDITION",
         "condition": {
            "condition_type": "AND",
            "statements": [
               {
                  "left": "${P::SCAN_LIST_OUTPUT{RESPONSE}
{SCAN_LIST}{SCAN}{REF}}",
                  "op": "!=",
                  "right": ""
               }
            ],
            "next": "END"
         }
      },
      {
         "name": "Debug#12",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "checkNetView",
         "operation": "CONDITION",
         "condition": {
            "condition_type": "OR",
            "statements": [
               {
                  "left": "${E::network.network_view}",
                  "op": "==",
                  "right": ""
               }
            ],
            "eval": "${XC:ASSIGN:{L:network_view}:{S:default}}",
            "else_eval": "${XC:COPY:{L:network_view}:
{E:network.network_view}}"
         }
      },
      {
         "name": "Debug#a",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
```

```
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "Get IPv4Fixed _ref",
      "operation": "GET",
      "transport": {
        "path": "fixedaddress?ipv4addr=${E:U:source_ip}
&network_view=${L:U:network_view}&_return_fields=extattrs"
      },
      "wapi": "v2.6"
    },
    {
      "name": "Debug#b",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "operation": "CONDITION",
      "name": "wapi_response_getIPv4Fix_ref",
      "condition": {
        "statements": [
          {
            "left": "${P:A:PARSE[0]{_ref}}",
            "op": "!=",
            "right": ""
          }
        ],
        "condition_type": "AND",
        "next": "Get_Objref"
      }
    },
    {
      "name": "Debug#c",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
         "name": "Get HostIPv4 _ref",
         "operation": "GET",
         "transport": {
            "path": "record:host?ipv4addr=${E:U:source_ip}&network_view=
${L:U:network_view}&_return_fields=extattrs"
         },
         "wapi": "v2.6"
      },
      {
         "name": "Debug#d",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "operation": "CONDITION",
         "name": "wapi_response_getIPv4Host_ref",
         "condition": {
            "statements": [
               {
                  "left": "${P:A:PARSE[0]{_ref}}",
                  "op": "!=",
                  "right": ""
               }
            ],
            "condition_type": "AND",
            "next": "Get_Objref"
         }
      },
      {
         "name": "Debug#e",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "StopHereBecauseNothingToUpdate",
         "operation": "CONDITION",
         "condition": {
            "statements": [
          {
            "left": "1",
            "op": "==",
            "right": "1"
          }
        ],
        "condition_type": "AND",
        "next": "launchVMscan"
      }
    },
    {
      "name": "Debug#f",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "Get_Objref",
      "operation": "CONDITION",
      "condition": {
        "statements": [
          {
            "left": "${P:A:PARSE[0]{_ref}}",
            "op": "!=",
            "right": ""
          }
        ],
        "condition_type": "AND",
        "eval": "${XC:COPY:{L:Obj_ref}:{P:PARSE[0]{_ref}}}"
      }
    },
    {
      "name": "Debug#g",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "CheckIfScannedToday",
      "operation": "CONDITION",
         "condition": {
            "statements": [
               {
                  "left": "${P:A:PARSE[0]{extattrs}{Qualys_LastScanTime}
{value}}",
                  "op": "==",
                  "right": "${L:A:ScanTime}"
               }
            ],
            "condition_type": "AND",
            "next": "END"
         }
      },
      {
         "name": "Debug#h",
         "operation": "NOP",
         "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
      },
      {
         "name": "launchVMscan",
         "operation": "POST",
         "transport": {
            "path": "/api/2.0/fo/scan/"
         },
         "parameters": [
            {
               "name": "action",
               "value": "launch"
            },
            {
               "name": "scan_title",
               "value": "${L:A:source_ip}+scan+initiated+by+Infoblox+at+
${UT::TIME}+by+a+${L:U:EventType}.+Domain:+${L:U:BlockedDomain}.
+RPZ+Rule+${L:U:RPZRule}."
            },
            {
               "name": "ip",
               "value": "${L:A:source_ip}"
            },
            {
```

```
          "name": "iscanner_name",
          "value": "${L:U:Qualys_Scanner}"
        },
        {
          "name": "option_title",
          "value": "${L:U:Qualys_Scan_Option}"
        }
      ],
      "parse": "XML"
    },
    {
      "name": "Debug#13",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "name": "checkScanStart",
      "operation": "CONDITION",
      "condition": {
        "condition_type": "OR",
        "statements": [
          {
            "left": "${P::SIMPLE_RETURN{RESPONSE}{CODE}}",
            "op": "==",
            "right": "1904"
          }
        ],
        "error": true
      }
    },
    {
      "name": "Debug#14",
      "operation": "NOP",
      "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:{UT:}}${XC:DEBUG:{R:}}"
    },
    {
      "operation": "CONDITION",
      "name": "Check if there is anything to update",
            "condition": {
                "statements": [
                    {
                        "left": "${L:A:Obj_ref}",
                        "op": "==",
                        "right": ""
                    }
                ],
                "condition_type": "AND",
                "next": "END"
            }
        },
        {
            "name": "Update Remediate Time",
            "operation": "PUT",
            "transport": {
                "path": "${L:A:Obj_ref}"
            },
            "wapi": "v2.6",
            "wapi_quoting": "JSON",
            "body_list": [
                "{",
                "\"extattrs+\":{\"Qualys_LastScanTime\": { \"value\":
\"${L:A:ScanTime}\"}}",
                "}"
            ]
        },
        {
            "name": "END",
            "operation": "NOP"
        },
        {
            "name": "Debug#15",
            "operation": "NOP",
            "body": "${XC:DEBUG:{H:}}${XC:DEBUG:{E:}}${XC:DEBUG:
{I:}}${XC:DEBUG:{L:}}${XC:DEBUG:{S:}}${XC:DEBUG:{P:}}${XC:DEBUG:
{UT:}}${XC:DEBUG:{R:}}"
        }
    ]
}
```