# SDN Firewall Auditing

Firewall auditing is a new capability for the SDN firewall in Windows Server 2019.  When enabled it records flows that are processed by SDN firewall rules (also known as ACLs) that have logging enabled to files on the hosts in a syntax that is consistent with the [Azure Network Watcher flow logs](https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview).   These logs can be used for diagnostics or archived for later analysis.  We will soon provide some examples of how to process these files using tools such as Power BI.

Please try it out and provide feedback!

Here is a sample script to enable firewall auditing on the Hyper-V hosts.  Update the variables at the beginning and run this on a Windows Server 2019 computer with the RSAT-NetworkController feature installed:

$logpath = "C:\test\log1"

$servers = @("sa18n22-2", "sa18n22-3", "sa18n22-4")

$uri = "<https://sa18n22sdn.sa18.nttest.microsoft.com>"

# Create log directories on the hosts

invoke-command -Computername $servers  {

    param(

        $Path

    )

    mkdir $path    -force

} -argumentlist $LogPath

# Set firewall auditing settings on Network Controller

$AuditProperties = new-object Microsoft.Windows.NetworkController.AuditingSettingsProperties

$AuditProperties.OutputDirectory = $logpath

set-networkcontrollerauditingsettingsconfiguration -connectionuri $uri -properties $AuditProperties -force  | out-null

# Enable logging on each server

$servers = get-networkcontrollerserver -connectionuri $uri

foreach ($s in $servers) {

    $s.properties.AuditingEnabled = @("Firewall")

    new-networkcontrollerserver -connectionuri $uri -resourceid $s.resourceid -properties $s.properties -force | out-null

}

Once enabled you will see a new file produced in the specified directory on each host about once per hour.    You should periodically process these files and remove them from the hosts.  The current file will have zero length and will be locked until flushed at the next hour mark:

PS C:\test\log1> dir

    Directory: C:\test\log1

Mode                LastWriteTime         Length Name

----                -------------         ------ ----

-a----        7/19/2018   6:28 AM          17055 SdnFirewallAuditing.d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a.20180719TL122803093.json

-a----        7/19/2018   7:28 AM           7880 SdnFirewallAuditing.d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a.20180719TL132803173.json

-a----        7/19/2018   8:28 AM           7867 SdnFirewallAuditing.d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a.20180719TL142803264.json

-a----        7/19/2018   9:28 AM          10949 SdnFirewallAuditing.d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a.20180719TL152803360.json

-a----        7/19/2018   9:28 AM              0 SdnFirewallAuditing.d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a.20180719TL162803464.json

These files will contain a sequence of flow events like this…

{

    "records": [

        {

            "properties":{

                "Version":"1.0",

                "flows":[

                    {

                        "flows":[

                            {

                                "flowTuples":["1531963580,192.122.0.22,192.122.255.255,138,138,U,I,A"],

                                "portId":"9",

                                "portName":"7290436D-0422-498A-8EB8-C6CF5115DACE"

                            }

                        ],

                        "rule":"Allow\_Inbound"

                    }

                ]

            },

            "operationName":"NetworkSecurityGroupFlowEvents",

            "resourceId":"394f647d-2ed0-4c31-87c5-389b8c0c8132",

            "time":"20180719:L012620622",

            "category":"NetworkSecurityGroupFlowEvent",

            "systemId":"d8b3b697-5355-40e2-84d2-1bf2f0e0dc4a"

            },

Etc...

Note, logging will only take place for rules that have Logging set to Enabled, for example:

{

    "Tags":  null,

    "ResourceRef":  "/accessControlLists/AllowAll",

    "InstanceId":  "4a63e1a5-3264-4986-9a59-4e77a8b107fa",

    "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",

    "ResourceMetadata":  null,

    "ResourceId":  "AllowAll",

    "Properties":  {

                       "ConfigurationState":  null,

                       "ProvisioningState":  "Succeeded",

                       "AclRules":  [

                                        {

                                            "ResourceMetadata":  null,

                                            "ResourceRef":  "/accessControlLists/AllowAll/aclRules/AllowAll\_Inbound",

                                            "InstanceId":  "ba8710a8-0f01-422b-9038-d1f2390645d7",

                                            "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",

                                            "ResourceId":  "AllowAll\_Inbound",

                                            "Properties":  {

                                                               "Protocol":  "All",

                                                               "SourcePortRange":  "0-65535",

                                                               "DestinationPortRange":  "0-65535",

                                                               "Action":  "Allow",

                                                               "SourceAddressPrefix":  "\*",

                                                               "DestinationAddressPrefix":  "\*",

                                                               "Priority":  "101",

                                                               "Description":  null,

                                                               "Type":  "Inbound",

                                                               "Logging":  "Enabled",

                                                               "ProvisioningState":  "Succeeded"

                                                           }

                                        },

                                        {

                                            "ResourceMetadata":  null,

                                            "ResourceRef":  "/accessControlLists/AllowAll/aclRules/AllowAll\_Outbound",

                                            "InstanceId":  "068264c6-2186-4dbc-bbe7-f504c6f47fa8",

                                            "Etag":  "W/\"1535a780-0fc8-4bba-a15a-093ecac9b88b\"",

                                            "ResourceId":  "AllowAll\_Outbound",

                                            "Properties":  {

                                                               "Protocol":  "All",

                                                               "SourcePortRange":  "0-65535",

                                                               "DestinationPortRange":  "0-65535",

                                                               "Action":  "Allow",

                                                               "SourceAddressPrefix":  "\*",

                                                               "DestinationAddressPrefix":  "\*",

                                                               "Priority":  "110",

                                                               "Description":  null,

                                                               "Type":  "Outbound",

                                                               "Logging":  "Enabled",

                                                               "ProvisioningState":  "Succeeded"

                                                           }

                                        }

                                    ],

                       "IpConfigurations":  [

                                            ],

                       "Subnets":  [

                                       {

                                           "ResourceMetadata":  null,

                                           "ResourceRef":  "/virtualNetworks/10\_0\_1\_0/subnets/Subnet1",

                                           "InstanceId":  "00000000-0000-0000-0000-000000000000",

                                           "Etag":  null,

                                           "ResourceId":  null,

                                           "Properties":  null

                                       }

                                   ]

                   }

}