Virtualization Implementation

Cisco AVS Distributed Firewall

About Cisco AVS Distributed Firewall

The Distributed Firewall is part of Cisco Application Virtual Switch (AVS) at the hypervisor kernel level and works in conjunction with the Cisco Application Centric Infrastructure (ACI) hardware for policy enforcement. The Distributed Firewall keeps track of the state of the network connection, traversing across it, and distinguishes legitimate packets for different types of TCP connection.

The Cisco AVS Distributed Firewall is completely assisted by Cisco ACI hardware. This combination of hardware and software provides greater performance and agility. In the Cisco ACI solution, leaf switches act as a policy store, which does not incur any performance penalty as the policies are processed in the hardware.

Distributed Firewall Behavior

In a Cisco ACI fabric, contracts using subjects and filters between consumer and provider EPGs are used to allow traffic. For example, the administrator creates a policy to allow traffic from any source port to destination port 80. As soon as the policy is configured in the Cisco Application Policy Infrastructure Controller (APIC), a reflexive ACL (access control list) entry from the provider to the consumer is automatically programmed in the Cisco ACI hardware. This reflexive ACL entry is necessary to allow the reverse traffic to flow. However, the leaf switch allows the provider (source port 80) to connect to any client destination port, which might not be desirable for some data centers. That is because endpoints in a provider EPG might initiate a SYN attack or a port-scan to the endpoints in the consumer EPGs using its source port 80.
The Distributed Firewall, with the help of the physical leaf switches, will not allow such SYN attacks. The leaf switch evaluates the packet and allows TCP packets only if the ACK flag is set, which prevents SYN attacks. Cisco AVS maintains the connection table to track the flow and allows TCP packets only if Cisco AVS has flow entry.

TCP Packets from Provider to Consumer

You can enable the Distributed Firewall feature on both the hardware leaf switch and Cisco AVS to prevent SYN attacks and SYN and ACK attacks from the provider.

The following figure illustrates how to prevent a SYN attack from the provider:
In this case, the following behavior occurs:

- If the SYN packets do not have the ACK bit set, then the hardware leaf switch drops the packets.
- If the SYN and ACK packets have the ACK bit set, then the hardware leaf permits the packets, but flow entry does not exist on AVS at the provider side. Therefore, Cisco AVS drops the packets.

The following figure illustrates how to prevent a SYN and ACK attack from the provider:

In this case, the following behavior occurs:

- If the data packets have the ACK bit set, then the hardware leaf switch permits the packets. If the connection is established, a flow entry exists on AVS. Therefore, the packets are permitted.
- If the RST packets have the ACK bit set, then they are handled similar to the data packets.
- If the FIN packets have the ACK bit set, then they are handled similar to the data packets. The FIN packets without the ACK bit set will be dropped by the hardware leaf switch.
The handling of FIN packets without the \texttt{ACK} bit set differs based on the type of the operating system, which enables such packets to be used for a FIN scan attack to determine the operating system. Dropping such packets can prevent this attack.

**Seamless FTP Traffic Handling**

The Distributed Firewall provides a stateful inspection capability for the FTP protocol. The Distributed Firewall snoops the FTP control connection (server TCP port 21) to get the data connection details (client IP and client port) and allows the FTP data connection (server TCP port 20) only for that flow. The Distributed Firewall supports only active FTP mode handling. No special handling is done for the passive FTP mode.

The following figure illustrates seamless FTP traffic handling:

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure5}
\caption{Seamless FTP Traffic Handling}
\end{figure}

**Guidelines and Limitations for Cisco AVS Distributed Firewall**

The following guidelines and limitations apply when using Cisco AVS Distributed Firewalls:

- Reflective ACL in the hardware is programmed to allow TCP packets only if the \texttt{ACK} flag is set.
- In receiving the first TCP SYN packet, Cisco AVS creates a flow table entry. The Cisco AVS drops packets if it does not have flow entry.
- Cisco AVS maintains the connection table to track the flow. Cisco AVS allows TCP packets only if it has flow entries.
- We recommend that you use vmxnet3 adapters for the VMs when using Distributed Firewall. We also recommend that you use vmxnet3 adapters in scale setups to increase the DVSLargeHeap size to its maximum (64 on 5.1 hosts and 128 on 5.5 hosts). You need to reboot the host for the change to take effect. For more information about using vmxnet3 adapters for scale setups, see the following VMware knowledge base article:

  Error message is displayed when a large number of dvPorts are in use in VMware ESXi 5.1.x (2034073).

**Configuration Examples for Cisco AVS Distributed Firewall Using the GUI**

You configure the Distributed Firewall by choosing one of the following modes:

- Enabled—Enforces the Distributed Firewall.
• Disabled—Does not enforce the Distributed Firewall. Use this mode only if you do not want to use the Distributed Firewall. Disabling the Distributed Firewall removes all flow information on the Cisco AVS.

• Learning—Cisco AVS monitors all TCP communication and creates flows in a flow table, but does not enforce the firewall. Learning is the default firewall mode in Cisco AVS Release 5.2(1)SV3(1.5) and Release 5.2(1)SV3(1.10). Learning mode provides a way to enable the firewall without losing traffic.

The following procedure provides an example of configuring the Cisco AVS Distributed Firewall with the Enabled mode using the advanced GUI mode.

Procedure

**Step 1**

Reflective ACL in the hardware is programmed to allow TCP packets only if the ACK flag is set. The following steps demonstrate how to configure a leaf switch to check the ACK flag:

a) On the menu bar, choose Tenants > tenant_name.

b) In the Navigation pane, expand tenant_name > Security Policies > Filters.

   The Security Policies - Filters panel appears in the Work pane. Your filters are displayed as rows inside a summary table.

c) Click the table row to display the Filter panel.

   The Entries table is displayed at the bottom of the Filter panel with a list of network traffic classification properties. To configure a leaf switch to check the ACK flag and allow TCP packets, the Stateful check box in the Entries table must be checked (set to True). By default, the Stateful check box is unchecked (set to False).

d) To check the Stateful check box, double-click on the row in the Entries table that represents the filter you want to configure. The filter will have tcp in the Protocol column and False in the Stateful column.

   The chosen row expands and enables you to edit the network traffic classification properties.

e) Put a check in the Stateful check box.

f) Click Update.

**Step 2**

In receiving the first TCP SYN packet, Cisco AVS creates a flow table entry. If Cisco AVS does not have a flow entry, it drops the packets. The following steps demonstrate how to configure Cisco AVS to enable the distributed firewall and maintain a connection table to track the flow:

a) On the menu bar, choose Fabric > Access Policies.

b) In the Navigation pane, choose Interface Policies > Policies > Firewall > default.

   The Firewall Policy - default panel appears.

c) In the Mode field, click the Enabled button. This property is referred to by VMM domain vSwitch policies. By default the Mode is Learning.

d) From the menu bar, choose VM NETWORKING > Inventory > VMware > ACI_AVS_name.

e) From the ACI_AVS_name pane, in the VSwitch Policy section, ensure the Firewall Policy field is default.

   If the Firewall Policy field is not set to default, you must be in the advanced GUI mode to change it.
TCP Packet Handling Example

The example below demonstrates how TCP packets are handled if the distributed firewall feature is enabled on both the leaf switches and the Cisco AVS (also see Configuration Examples for Cisco AVS Distributed Firewall Using the GUI, on page 4).

If the SYN packets do not have the ACK bit set, the leaf switch drops the packets. If the SYN and ACK packets have the ACK bit set, the leaf switch permits the packets, but the flow entry does not exist on Cisco AVS at the provider side. This causes the Cisco AVS to drop the packets.

*Figure 6: Prevent SYN attack from Provider*

If the data packets have the ACK bit set, the leaf switch permits the packets. If the connection is established, a flow entry exists on Cisco AVS and the packets are permitted. If the RST packets also have the ACK bit set, they are handled similarly to the data packets.

FIN packets with the ACK bit set are also handled similarly to the data packets. The FIN packets without the ACK bit set are dropped by the leaf switch.
• The handling of FIN packets without the ACK bit set differs based on the type of the operating system. So it can be used for FIN scan attacks to determine the operating system.
• Dropping FIN packets without the ACK bit set can prevent such an attack.

FTP Traffic Handling Example

Distributed firewall provides a stateful inspection capability for FTP. Distributed firewall snoops the FTP control connection (Server TCP port 21) to get the data connection details (client IP and client port) and to allow the FTP data connection (Server TCP port 20) only for that flow. Support is only for active-FTP mode handling. No special handling will be done for passive-FTP mode.

Additional References for Cisco AVS Distributed Firewall

For more information on AVS Distributed Firewalls, see the Cisco ACI Virtualization Guide at the following URL:
