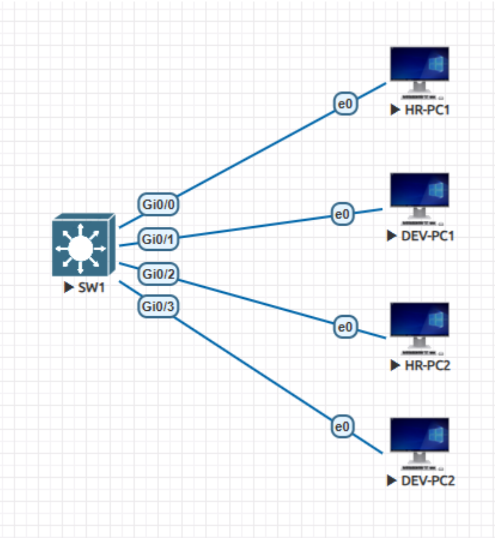
Layer 2 Traffic Isolation

Let’s imagine we are designing the network for a company, and we’re not very good at our job! We solve issues as they arise one by one, rather than predicting them in advance. This poor approach here will give us a chance to explain how various concepts are related, but designed to solve different problems.

To start, we have people from HR and Development teams on the first floor, and each department has its own printer and workstations. Naturally, we wouldn’t want people from HR to print to the Development printer, or a developer’s workstation to have reachability to an HR workstation. What do we do? Well, one solution could be to buy two switches and put HR devices and printer on one, and Development devices and printer on the other. With no links between the two switches, we get what we want. Any problems with this approach? It’s not very scalable among other things. If we add a few other departments, we will need more switches – which can get very pricey very quickly. Plus, there will be a lot of wasted ports! If HR has only 4 people and 1 printer, other ports on their switch will be left empty. So overall, not a feasible way to solve our problem.

Fortunately for us, smart people came up with a much better solution. They invented Virtual LANs. These pieces of magic give us the same separation that we created above, but on the same switch. We create different VLANs for different departments and then connect devices to appropriate ports. Even though all devices are connected to the same physical switch, traffic isolation is there. Better? Most definitely. Ideal? Well, we will still need to deal with issues such as preventing people from connecting their workstation to a port in another VLAN, or what to do if someone from HR wants to work from the second floor instead of the first floor, etc., but we will not address such difficulties here. So for now, we have successfully separated HR traffic from Development traffic.

Let’s quickly see this in action. I’ll use the following topology to illustrate the point and highlight important sections in the configuration (e.g. key configuration, show commands, output sections, etc.)



```
SW1(config)#vlan 20
SW1(config-vlan)#name HR
SW1(config-vlan)#vlan 30
SW1(config-vlan)#name DEVELOPMENT

SW1(config-vlan)#interface g0/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20

SW1(config-if)#interface g0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
```

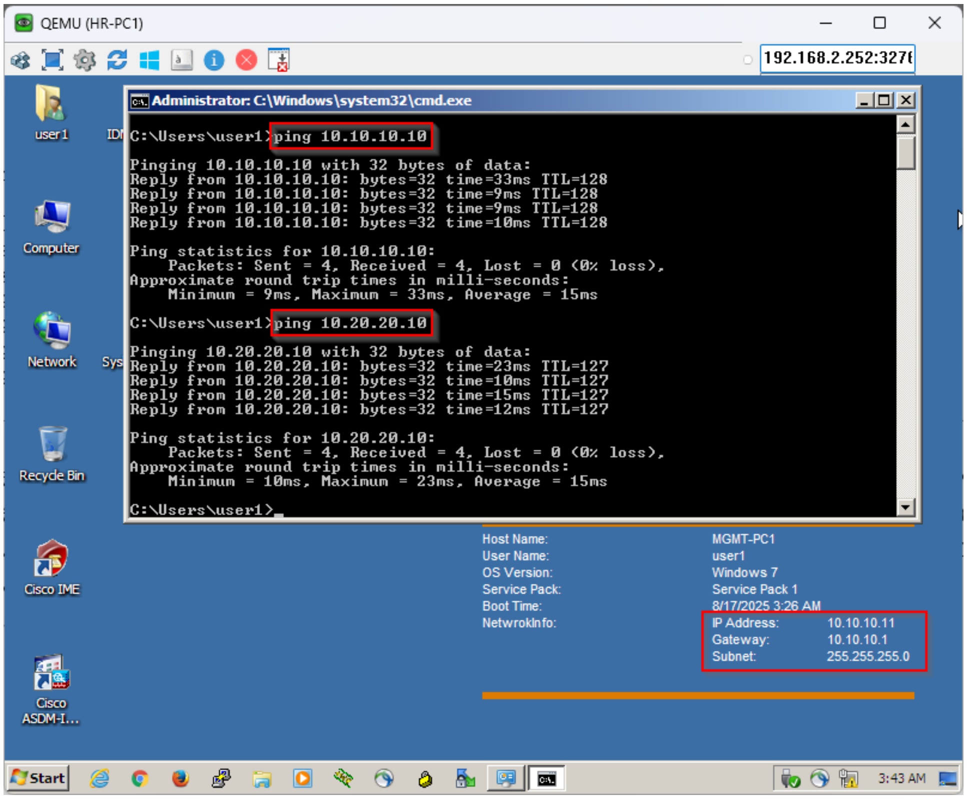
```
SW1(config-if)#interface g0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30

SW1(config-if)#interface g0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30

SW1(config-if)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0, Gi1/1, Gi1/2, Gi1/3
20   HR                               active    Gi0/0, Gi0/2
30   DEVELOPMENT                      active    Gi0/1, Gi0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

To communicate, our devices need IP addresses. I can assign them statically as I only have 4 hosts, but I'll quickly configure DHCP on the switch to make it a bit more interesting. To do this, I will create two DHCP pools (HR_POOL and DEV_POOL) and use VLAN interfaces as default gateways. It is a best practice to exclude the addresses that you don't want assigned to hosts before you create the pools.

```
SW1(config)#ip dhcp excluded-address 10.10.10.1 10.10.10.9
SW1(config)#ip dhcp excluded-address 10.20.20.1 10.20.20.9

SW1(config)#ip dhcp pool HR_POOL
SW1(dhcp-config)#network 10.10.10.0 ?
  /nn or A.B.C.D  Network mask or prefix length
  <cr>
SW1(dhcp-config)#network 10.10.10.0 /24
SW1(dhcp-config)#default-router 10.10.10.1

SW1(config)#ip dhcp pool DEV_POOL
SW1(dhcp-config)#network 10.20.20.0 /24
SW1(dhcp-config)#default-router 10.20.20.1

SW1(dhcp-config)#int vlan 20
SW1(config-if)#ip add 10.10.10.1 255.255.255.0

SW1(config-if)#int vlan 30
SW1(config-if)#ip add 10.20.20.1 255.255.255.0

SW1#show ip dhcp pool

Pool HR_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 9
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.10.10.12          10.10.10.1       - 10.10.10.254      0     / 9     / 254

Pool DEV_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 9
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 10.20.20.12         10.20.20.1       - 10.20.20.254      0     / 9     / 254

SW1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address       Client-ID/              Lease expiration        Type       State      Interface
                 Hardware address/
                 User name
10.10.10.10       0150.0000.0f00.00       Aug 18 2025 02:37 AM    Automatic  Active     Vlan20
10.10.10.11       0150.0000.0d00.00       Aug 18 2025 02:37 AM    Automatic  Active     Vlan20
10.20.20.10       0150.0000.0e00.00       Aug 18 2025 02:37 AM    Automatic  Active     Vlan30
10.20.20.11       0150.0000.1000.00       Aug 18 2025 02:37 AM    Automatic  Active     Vlan30
```

Looks good! One point to draw attention to, though, and that is the relationship between VLAN number and IP address range used in conjunction with it. As you can see above, I used the 10.10.10.0/24 network for VLAN 20 and the 10.20.20.0/24 for VLAN 30. The VLAN number has nothing to do with the address range, but it makes every sense to use a combination that is less confusing than what I used here! VLAN 20 would have made more sense with 10.20.20.0/24, but I was trying to make a point!

OK, time to test. Hopefully, devices in the 10.10.10.0/24 range should be able to reach each other, but not the 10.20.20.0/24 devices.



```
C:\Users\user1>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=33ms TTL=128
Reply from 10.10.10.10: bytes=32 time=9ms TTL=128
Reply from 10.10.10.10: bytes=32 time=9ms TTL=128
Reply from 10.10.10.10: bytes=32 time=10ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 33ms, Average = 15ms

C:\Users\user1>ping 10.20.20.10

Pinging 10.20.20.10 with 32 bytes of data:
Reply from 10.20.20.10: bytes=32 time=23ms TTL=127
Reply from 10.20.20.10: bytes=32 time=10ms TTL=127
Reply from 10.20.20.10: bytes=32 time=15ms TTL=127
Reply from 10.20.20.10: bytes=32 time=12ms TTL=127

Ping statistics for 10.20.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 23ms, Average = 15ms

C:\Users\user1>_
```

Host Name:	MGMT-PC1
User Name:	user1
OS Version:	Windows 7
Service Pack:	Service Pack 1
Boot Time:	8/17/2025 3:26 AM
NetwrokInfo:	IP Address: 10.10.10.11 Gateway: 10.10.10.1 Subnet: 255.255.255.0

Wait – what? Well, this is because I used VLAN interfaces, essentially turning my switch into a router.

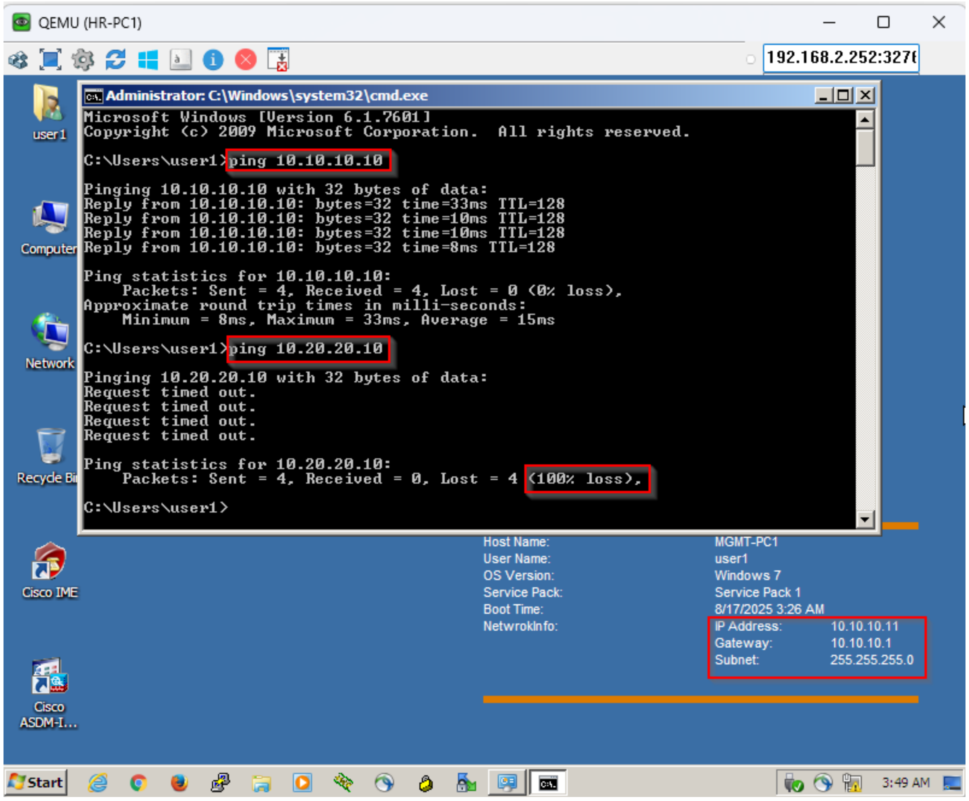
```
SW1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Vlan20
L        10.10.10.1/32 is directly connected, Vlan20
C        10.20.20.0/24 is directly connected, Vlan30
L        10.20.20.1/32 is directly connected, Vlan30
```

Traffic here is being routed at layer 3 between VLANs. Let’s see if we can fix this.

```
SW1(config)#no ip routing
SW1(config)#do sh ip route
Default gateway is not set

Host                  Gateway           Last Use    Total Uses  Interface
ICMP redirect cache is empty

SW1(config)#do sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  up                    up
GigabitEthernet1/3     unassigned      YES unset  up                    up
Vlan20                 10.10.10.1      YES manual up                    up
Vlan30                 10.20.20.1      YES manual up                    up
```

And if we try the pings again,

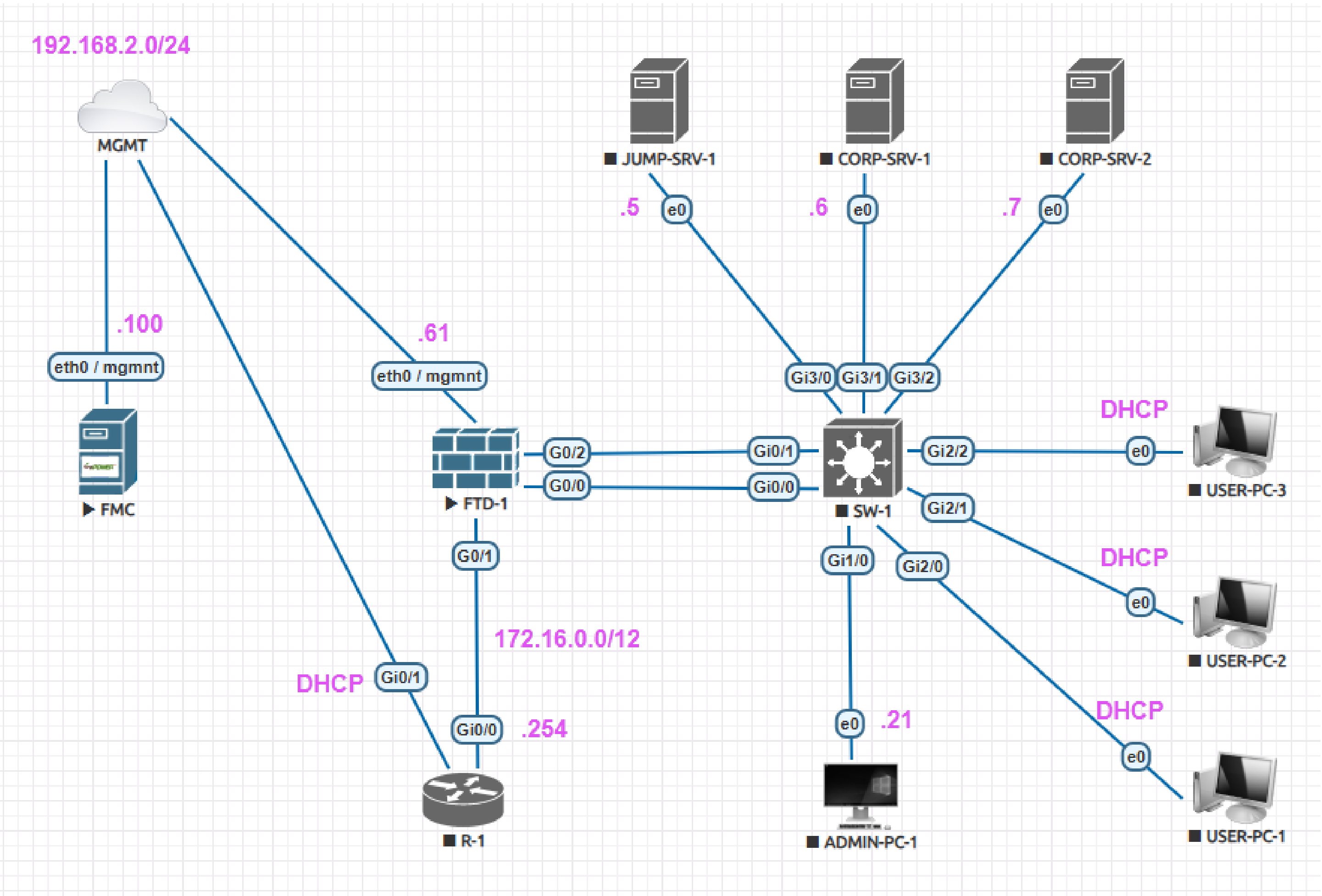


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user1>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=33ms TTL=128
Reply from 10.10.10.10: bytes=32 time=10ms TTL=128
Reply from 10.10.10.10: bytes=32 time=10ms TTL=128
Reply from 10.10.10.10: bytes=32 time=8ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 33ms, Average = 15ms

C:\Users\user1>ping 10.20.20.10

Pinging 10.20.20.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.20.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user1>
```

```
Host Name:          MGMT-PC1
User Name:          user1
OS Version:         Windows 7
Service Pack:       Service Pack 1
Boot Time:          8/17/2025 3:26 AM
NetwrokInfo:        IP Address:   10.10.10.11
                    Gateway:      10.10.10.1
                    Subnet:       255.255.255.0
```

OK, much better! I won’t paste the screenshots, but the same connectivity pattern applies to our other hosts as well. Just take my word for it.

As soon as we begin to enjoy our little victory here, things take a twist. Our boss says that we are adding a few servers for the development team, but we don't want the team to directly access the corporate servers. All access should be via a jump server. This is an entirely different type of challenge, no? Previously, we were trying to isolate people and devices in one department from people and devices in another department. Now, we need to isolate things inside the same department! If everything is in the same VLAN, everything can reach everything else by default. What do we do now? I'll switch to a different topology for this (and future) scenarios. We will remove HR from our picture and focus solely on the development team.



For now, ignore the Firepower Threat Defense and Firepower Management Center. Let's start by configuring our switch and IP addressing.

```
SW-1(config)#vlan 20
SW-1(config-vlan)#name DEVELOPMENT

SW-1(config-vlan)#int range g3/0-2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20

SW-1(config-if-range)#int range g2/0-2
SW-1(config-if-range)#switchport mode access
SW-1(config-if-range)#switchport access vlan 20

SW-1(config-if-range)#int g1/0
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 20
SW-1(config-if)#exit

SW-1(config)#ip dhcp excluded-address 10.20.20.1 10.20.20.30
```

```
SW-1(config)#ip dhcp pool DEV_POOL
SW-1(dhcp-config)#network 10.20.20.0 /24

SW-1(dhcp-config)#interface vlan 20
SW-1(config-if)#ip address 10.20.20.1 255.255.255.0
SW-1(config-if)#do wr
```

I'll assign static IP addresses to the servers and admin PC in the same 10.20.20.0 /24 range. As expected, all devices have reachability to each other as they are in the same VLAN and configured with IP addresses in the same range.

Now let's address our new challenge. Based on the diagram above (and ignoring the Admin PC for now), we have been asked to make sure that:

- There is bidirectional connectivity between all devices and JUMP-SRV-1
- There is no connectivity between any USER-PC and CORP-SRV-1 or CORP-SRV-2

To implement this, we need a technology that allows for intra-VLAN (as opposed to inter-VLAN) traffic isolation. One such technology as VLAN Access-lists (or VACLs). To use these, the first step is to identify the "interesting" traffic (i.e. the traffic we need to work with) using an ACL. Then we will define what to do with the said traffic in a VLAN access-map.

```
SW-1(config)#ip access-list extended BLK_PC2CORP
SW-1(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 host 10.20.20.6
SW-1(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 host 10.20.20.7
SW-1(config-ext-nacl)#exit

SW-1(config)#vlan access-map ?
  WORD  Vlan access map tag

SW-1(config)#vlan access-map DEV_ACCMAP ?
  <0-65535>  Sequence to insert to/delete from existing vlan access-map entry
  <cr>

SW-1(config)#vlan access-map DEV_ACCMAP 10
SW-1(config-access-map)#?
Vlan access-map configuration commands:
  action   Take the action
  default  Set a command to its defaults
  exit     Exit from vlan access-map configuration mode
  match    Match values.
  no       Negate a command or set its defaults

SW-1(config-access-map)#match ?
  ip    IP based match
  ipv6  IPv6 based match
  mac   MAC based match

SW-1(config-access-map)#match ip ?
  address  Match IP address to access control.

SW-1(config-access-map)#match ip address ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD         Access-list name

SW-1(config-access-map)#match ip address BLK_PC2CORP
SW-1(config-access-map)#action ?
  drop     Drop packets
  forward  Forward packets

SW-1(config-access-map)#action drop
```

```
SW-1(config-access-map)#vlan access-map DEV_ACCMAP 20
SW-1(config-access-map)#action forward
SW-1(config-access-map)#do wr
```

A point that might seem confusing at first is the “permit” action used in our access-list. As I mentioned, the access-list’s job is only to identify the traffic, not to take any action on it; therefore, in this context, “permit” simply means “include” and “deny” would mean “exclude.” The action is defined using the VLAN access-map.

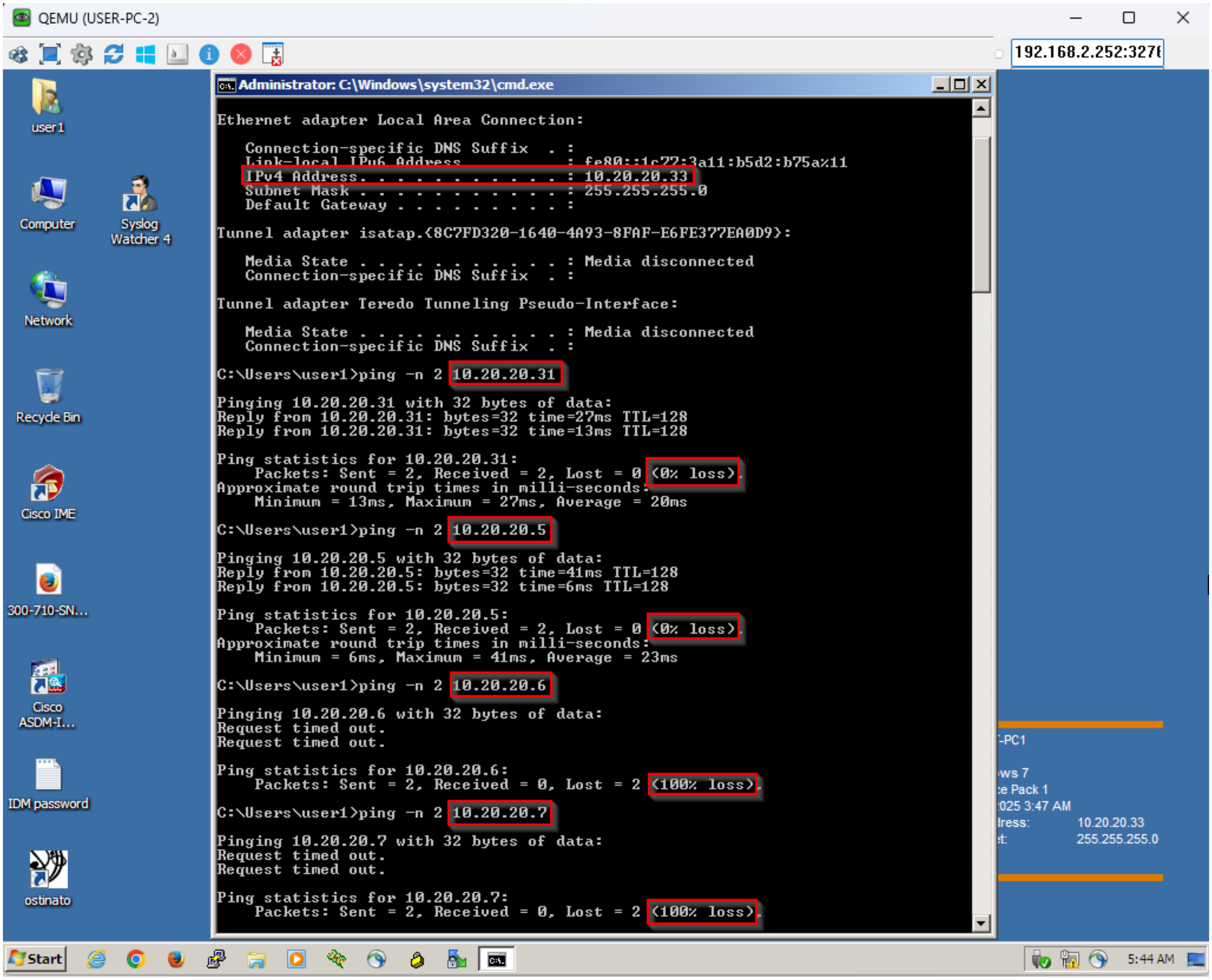
So, what have we done so far? We have identified traffic from any device in the 10.20.20.0 /24 going to 10.20.20.6 or 10.20.20.7; we have identified an action to be taken again this traffic; but we have not applied these anywhere. Just like a normal ACL has to be applied somewhere (usually an interface), a VACL needs to be applied somewhere as well – to a VLAN. Proof that nothing is happening despite our lengthy configuration above comes from the fact that our access-list has no hit counts no matter how many pings we run among our devices.

```
SW-1(config)#do sh ip access-list
Extended IP access list BLK_PC2CORP
    10 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.6
    20 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.7
```

So, how do we apply the access-map to a VLAN? We use a VLAN filter. We tell our switch to apply the access-map we created before to vlan 20 as a filter.

```
SW-1(config)#vlan filter ?
  WORD  VLAN map name

SW-1(config)#vlan filter DEV_ACCMAP ?
  vlan-list  VLANs to apply filter to

SW-1(config)#vlan filter DEV_ACCMAP vlan-list ?
  <1-4094>  VLAN id
  all       Add this filter to all VLANs

SW-1(config)#vlan filter DEV_ACCMAP vlan-list 20
```

Let’s test – from our PC at 10.20.20.33 to another PC at 10.20.20.31, and then to our servers at 10.20.20.5, 10.20.20.6, and 10.20.20.7.

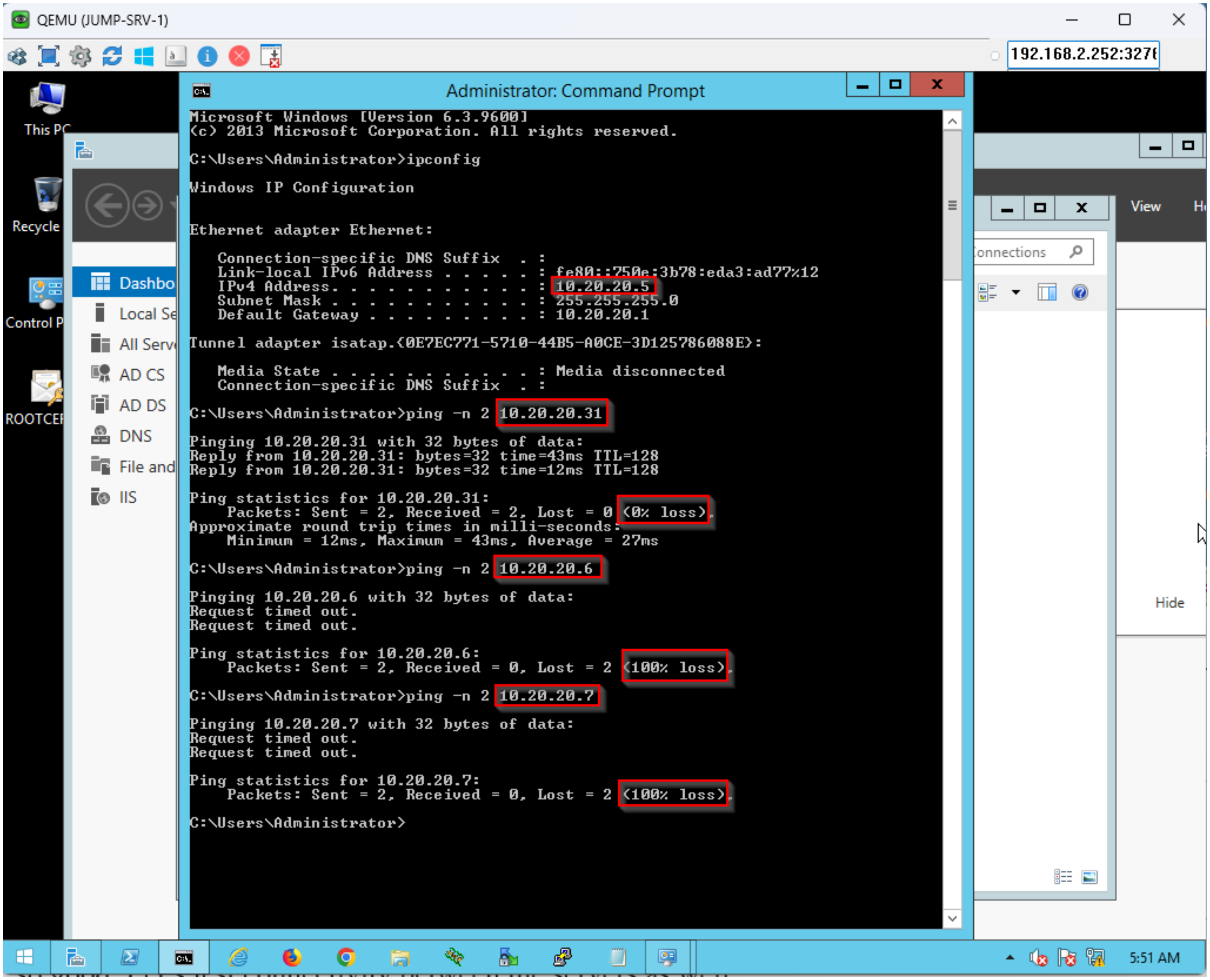


```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c77:3a11:b5d2:b75a%11
   IPv4 Address. . . . . . . . . . . : 10.20.20.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{8C7FD320-1640-4A93-8FAF-E6FE377EA0D9}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user1>ping -n 2 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.31: bytes=32 time=27ms TTL=128
Reply from 10.20.20.31: bytes=32 time=13ms TTL=128

Ping statistics for 10.20.20.31:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 27ms, Average = 20ms

C:\Users\user1>ping -n 2 10.20.20.5

Pinging 10.20.20.5 with 32 bytes of data:
Reply from 10.20.20.5: bytes=32 time=41ms TTL=128
Reply from 10.20.20.5: bytes=32 time=6ms TTL=128

Ping statistics for 10.20.20.5:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 41ms, Average = 23ms

C:\Users\user1>ping -n 2 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.20.20.6:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss).

C:\Users\user1>ping -n 2 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.20.20.7:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss).
```

OK – it looks like we have achieved something. Our PC has lost connectivity to both corporate servers, but not to other PCs or the jump server. Our switch also now confirms the 2 dropped pings to these two corporate servers:

```
SW-1(config)#do sh ip access-list
Extended IP access list BLK_PC2CORP
    10 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.6 (2 matches)
    20 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.7 (2 matches)
```

So far, so good. Let's test connectivity between the servers as well. Afterall, part of our requirement is to allow access to the corporate servers via the jump server.



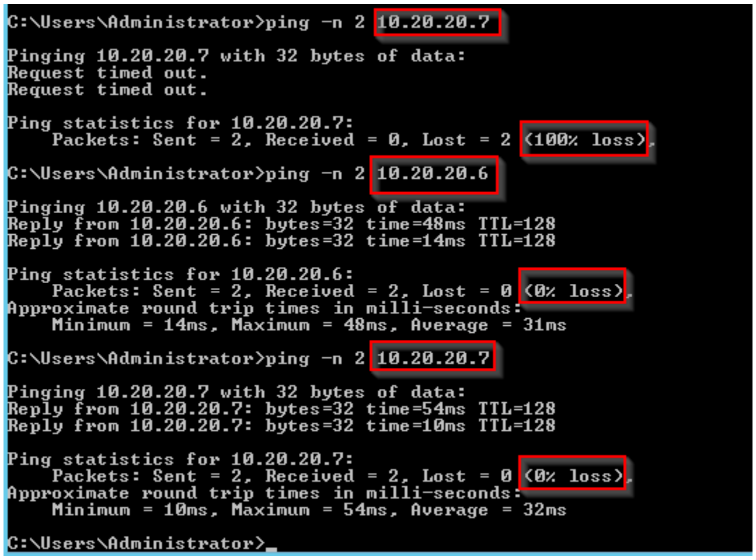
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::750e:3b78:eda3:ad77%12
   IPv4 Address. . . . . . . . . . . : 10.20.20.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.20.1

Tunnel adapter isatap.{0E7EC771-5710-44B5-A0CE-3D125786088E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>ping -n 2 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.31: bytes=32 time=43ms TTL=128
Reply from 10.20.20.31: bytes=32 time=12ms TTL=128

Ping statistics for 10.20.20.31:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 43ms, Average = 27ms

C:\Users\Administrator>ping -n 2 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.20.20.6:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

C:\Users\Administrator>ping -n 2 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.20.20.7:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

C:\Users\Administrator>
```

Uh-oh! Well, I'd say this was expected as we didn't take any steps to somehow exclude our jump server at 10.20.20.5 from whatever fate we were creating for traffic coming from 10.20.20.0 /24 to our corporate servers. Let's see if we can use a "deny" statement in our access-list to "exclude" this specific traffic. Note that I will add the new entries above our previous entries, using lower sequence numbers.

```
SW-1(config)#ip access-list extended BLK_PC2CORP
SW-1(config-ext-nacl)#5 deny ip host 10.20.20.5 host 10.20.20.6
SW-1(config-ext-nacl)#7 deny ip host 10.20.20.5 host 10.20.20.7
SW-1(config-ext-nacl)#do wr
```

And another test!

```
SW-1(config-ext-nacl)#do sh ip access-list
Extended IP access list BLK_PC2CORP
    5 deny ip host 10.20.20.5 host 10.20.20.6 (2 matches)
    7 deny ip host 10.20.20.5 host 10.20.20.7 (2 matches)
    10 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.6 (4 matches)
    20 permit ip 10.20.20.0 0.0.0.255 host 10.20.20.7 (4 matches)
```



```
C:\Users\Administrator>ping -n 2 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 10.20.20.7:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

C:\Users\Administrator>ping -n 2 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Reply from 10.20.20.6: bytes=32 time=48ms TTL=128
Reply from 10.20.20.6: bytes=32 time=14ms TTL=128

Ping statistics for 10.20.20.6:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 48ms, Average = 31ms

C:\Users\Administrator>ping -n 2 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Reply from 10.20.20.7: bytes=32 time=54ms TTL=128
Reply from 10.20.20.7: bytes=32 time=10ms TTL=128

Ping statistics for 10.20.20.7:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 54ms, Average = 32ms

C:\Users\Administrator>_
```

We're back in business. However, hopefully, you see that this is not a scalable solution. To allow access from the jump server to other servers, a separate entry needs to be added every time, and we completely ignored reachability between the corporate servers themselves. It can become confusing and cumbersome to maintain very quickly. But for now, our boss is happy – albeit temporarily! Here he is with another challenge for us.

We will be adding more corporate servers soon, and our boss wants us to make sure access will be seamless – no direct access from the workstations to any of the corporate servers except via the jump server. Well, unfortunately for us, this is aiming straight for that scalability issue we just discussed above! We need a new solution. And behold – Private VLANs!

Private VLANs and VACLs are normally not used together. So, I'll "retire" our old configuration and get us back to full reachability between all devices. Then I'll start with our new solution.

```
SW-1(config)#no vlan filter DEV_ACCMAP vlan-list 20
SW-1(config)#no vlan access-map DEV_ACCMAP 10
SW-1(config)#no vlan access-map DEV_ACCMAP 20
SW-1(config)#no ip access-list extended BLK_PC2CORP
SW-1(config)#do wr
Building configuration...
Compressed configuration from 3883 bytes to 1791 bytes[OK]
SW-1(config)#
*Aug 17 08:46:24.026: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Aug 17 08:46:25.082: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
SW-1(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                Gi1/1, Gi1/2, Gi1/3, Gi2/3
                                                Gi3/3
20   DEVELOPMENT                      active    Gi1/0, Gi2/0, Gi2/1, Gi2/2
                                                Gi3/0, Gi3/1, Gi3/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Let's start by creating a new VLAN for our Development team, this time paying more attention to the options we have at our disposal when creating it.

```
SW-1(config)#vlan 50
SW-1(config-vlan)#?
VLAN configuration commands:
  are           Maximum number of All Route Explorer hops for this VLAN (or
                zero if none specified)
  backupcrf     Backup CRF mode of the VLAN
  bridge        Bridging characteristics of the VLAN
  exit          Apply changes, bump revision number, and exit mode
  media         Media type of the VLAN
  mtu           VLAN Maximum Transmission Unit
  name          Ascii name of the VLAN
  no            Negate a command or set its defaults
  parent        ID number of the Parent VLAN of FDDI or Token Ring type VLANs
  private-vlan  Configure a private VLAN
  remote-span   Configure as Remote SPAN VLAN
  ring          Ring number of FDDI or Token Ring type VLANs
  said          IEEE 802.10 SAID
  shutdown      Shutdown VLAN switching
  state         Operational state of the VLAN
  ste           Maximum number of Spanning Tree Explorer hops for this VLAN (or
                zero if none specified)
  stp           Spanning tree characteristics of the VLAN
  tb-vlan1      ID number of the first translational VLAN for this VLAN (or
                zero if none)
  tb-vlan2      ID number of the second translational VLAN for this VLAN (or
                zero if none)

SW-1(config-vlan)#private-vlan ?
  association       Configure association between private VLANs
  community         Configure the VLAN as a community private VLAN
  isolated          Configure the VLAN as an isolated private VLAN
  primary           Configure the VLAN as a primary private VLAN
  twoway-community  Configure the VLAN as a two way community private VLAN

SW-1(config-vlan)#private-vlan primary ?
  <cr>

SW-1(config-vlan)#private-vlan primary
%Private VLANs can only be configured when VTP is in transparent/off modes in VTP version 1 or 2 and in
server/transparent/off modes in VTP version 3 when pruning is turned off

SW-1(config-vlan)#do sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 5000.0004.8000
Configuration last modified by 0.0.0.0 at 8-17-25 03:27:53
Local updater ID is 10.20.20.1 on interface Vl20 (lowest numbered VLAN interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 6
Configuration Revision            : 3
MD5 digest                        : 0xFC 0xCB 0xBE 0x52 0x9A 0x4C 0x85 0x25
                                    0x9F 0x2B 0xAE 0x0E 0xE2 0x6A 0x41 0xB2
```

OK – so, we need to solve the VTP issue before we can get back to our Private VLAN configuration.

```
SW-1(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
SW-1(config)#do sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
```

```
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 5000.0004.8000
Configuration last modified by 10.20.20.1 at 8-17-25 09:03:36

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 0
MD5 digest                        : 0x03 0x7F 0x04 0x01 0x21 0xA4 0x74 0x67
                                    0x4A 0x5F 0x91 0xE1 0x56 0x75 0x47 0x00
```

Back to Private VLANs.

```
SW-1(config)#vlan 50
SW-1(config-vlan)#private-vlan primary
SW-1(config-vlan)#name DEV_PRIM_VLAN

SW-1(config-vlan)#vlan 501
SW-1(config-vlan)#name DEV_ISO_VLAN
SW-1(config-vlan)#private-vlan isolated

SW-1(config-vlan)#vlan 502
SW-1(config-vlan)#name DEV_COM_VLAN
SW-1(config-vlan)#private-vlan community

SW-1(config-vlan)#exit
SW-1(config)#do sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                Gi1/1, Gi1/2, Gi1/3, Gi2/3
                                                Gi3/3
20   DEVELOPMENT                      active    Gi1/0, Gi2/0, Gi2/1, Gi2/2
                                                Gi3/0, Gi3/1, Gi3/2
50   DEV_PRIM_VLAN                    active
501  DEV_ISO_VLAN                     active
502  DEV_COM_VLAN                     active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

OK, I'm sure you expect a bit of explanation before we go on. VLAN 50 is our primary VLAN – think of it as the main container. We also have two "secondary" VLANs 501 and 502 (names are purely arbitrary!), configured as isolated and community respectively. Isolated VLANs do not allow communication between any of the hosts inside them, hence the name! Community VLANs allow mutual communication inside. Now, our switch knows that these three VLANs exist, but it doesn't know that we want VLAN 501 and VLAN 502 to be associated with VLAN 50. Let's fix this.

```
SW-1(config)#vlan 50
SW-1(config-vlan)#private-vlan association ?
  WORD    VLAN IDs of the private VLANs to be configured
  add     Add a VLAN to private VLAN list
  remove  Remove a VLAN from private VLAN list

SW-1(config-vlan)#private-vlan association 501,502

SW-1(config-vlan)#do sh vlan br

VLAN Name                             Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                Gi1/1, Gi1/2, Gi1/3, Gi2/3
                                                Gi3/3
20   DEVELOPMENT                      active    Gi1/0, Gi2/0, Gi2/1, Gi2/2
                                                Gi3/0, Gi3/1, Gi3/2
50   DEV_PRIM_VLAN                    active
501  DEV_ISO_VLAN                     active
502  DEV_COM_VLAN                     active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Although our list of VLANs above seems unaffected, we can see confirmation of what we did below.

```
SW-1(config-vlan)#do sh vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
50      none      primary
none    501       isolated
none    502       community
```

Now our switch knows that the three VLANs are linked. What's next? We need to assign ports to these VLANs. Right now, all of our ports are in VLAN 20, that we created before. Before we make any changes, though, let's see what ports need to be in what type of VLAN. Based on our requirements, we want developers to be able to talk to each other; so, we can put them all in a community VLAN. We could also put all corporate servers in another community VLAN (which I did not create), since members of a community can only talk to each other, not members of another community. However, to prevent servers from launching attacks on each other, it's probably a better security practice to isolate them from each other as well as from user devices. Therefore, we will put the servers in our isolated VLAN. What about the jump server? We want all other hosts to be able to reach it. I'll show you what to do with it when the time comes!

```
SW-1(config)#interface range g2/0-2
SW-1(config-if-range)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally

SW-1(config-if-range)#switchport mode private-vlan ?
  host         Set the mode to private-vlan host
  promiscuous  Set the mode to private-vlan promiscuous
  trunk        Set the mode to private-vlan trunk

SW-1(config-if-range)#switchport mode private-vlan host
SW-1(config-if-range)#switchport private-vlan association ?
  host   Set the private VLAN host association
  trunk  Set the private VLAN trunk association

SW-1(config-if-range)#switchport private-vlan host-association ?
  <1006-4094>  Primary extended range VLAN ID of the private VLAN host port
               association
  <2-1001>     Primary normal range VLAN ID of the private VLAN port
               association

SW-1(config-if-range)#switchport private-vlan host-association 50 ?
  <1006-4094>  Secondary extended range VLAN ID of the private VLAN host port
               association
  <2-1001>     Secondary normal range VLAN ID of the private VLAN host port
               association
```

```
SW-1(config-if-range)#switchport private-vlan host-association 50 502 ?
  <cr>

SW-1(config-if-range)#switchport private-vlan host-association 50 502
```

Not bad! The principle is quite similar to how we configure a normal port on the switch. We need to choose what “mode” the port runs in (e.g. access vs. trunk), and the mode in this case is private-vlan host. Then we need to configure the VLAN, but in our case, it’ll be 2 VLANs – one primary and one secondary. So now, all our PCs should still be able to talk with each other, but not to anything else. Access to interface VLAN 20 is no longer there, but the devices still have their IP addresses. At some point, I’ll need to provide a new DHCP, though. Moving on to the servers.

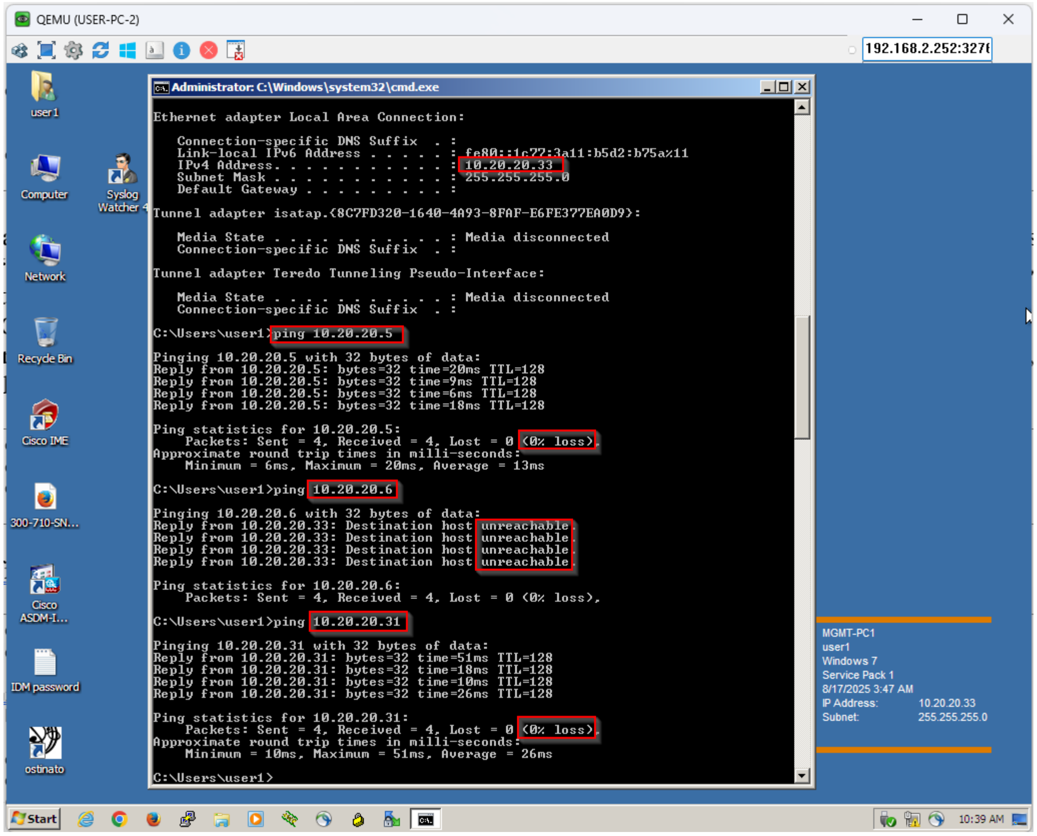
```
SW-1(config)#interface range g3/1-2
SW-1(config-if-range)#switchport mode private-vlan host
SW-1(config-if-range)#switchport private-vlan host-association 50 501
```

And finally time for the jump server! This will be slightly different.

```
SW-1(config-if-range)#int g3/0
SW-1(config-if)#switchport mode private-vlan ?
  host         Set the mode to private-vlan host
  promiscuous  Set the mode to private-vlan promiscuous
  trunk        Set the mode to private-vlan trunk

SW-1(config-if)#switchport mode private-vlan promiscuous
SW-1(config-if)#switchport private-vlan ?
  association       Set the private VLAN association
  host-association  Set the private VLAN host association
  mapping           Set the private VLAN promiscuous mapping
  trunk             Set the private vlan trunking configuration

SW-1(config-if)#switchport private-vlan mapping ?
  <1006-4094>  Primary extended range VLAN ID of the private VLAN promiscuous
               port mapping
  <2-1001>     Primary normal range VLAN ID of the private VLAN promiscuous
               port mapping

SW-1(config-if)#switchport private-vlan mapping 50 ?
  WORD    Secondary VLAN IDs of the private VLAN promiscuous port mapping
  add     Add a VLAN to private VLAN list
  remove  Remove a VLAN from private VLAN list

SW-1(config-if)#switchport private-vlan mapping 50 501,502
```

The mode will be set to promiscuous, and the mapping will include the primary VLAN and all other secondary VLANs (they all need to be able to communicate with this promiscuous port, remember?) OK, testing time!

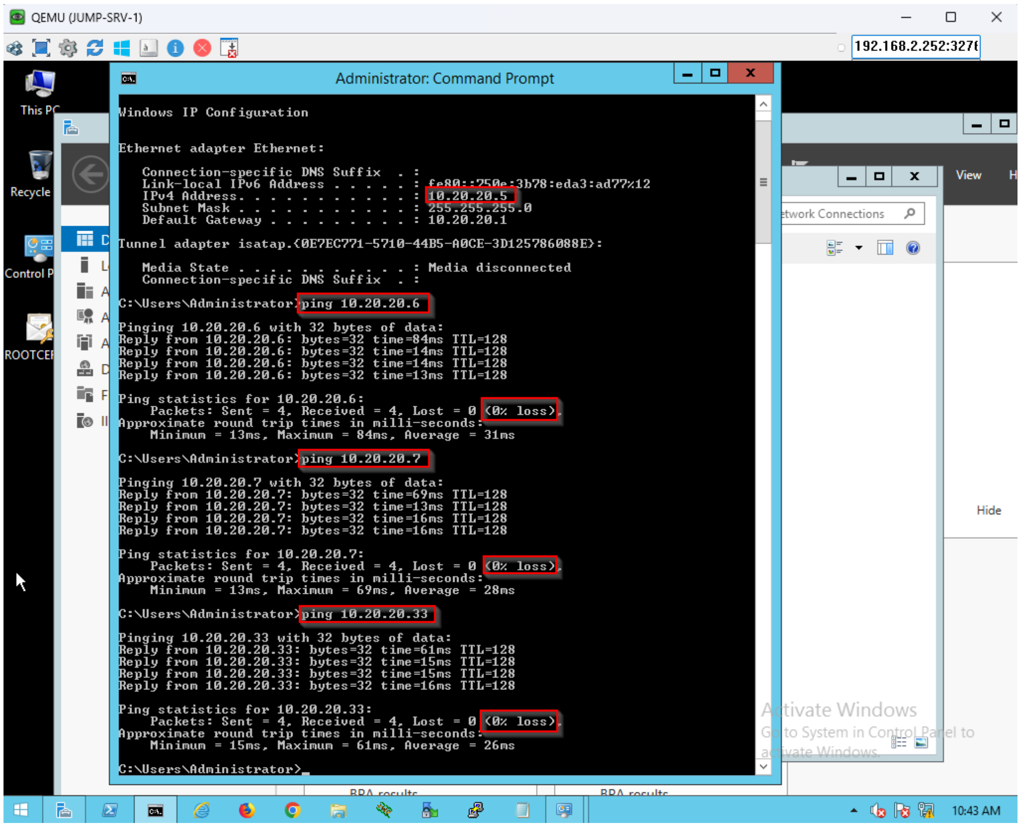
In our first test, we see reachability from a PC to other PCs and jump server, but not the corporate server.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c77:3a11:b5d2:b75a%11
   IPv4 Address. . . . . . . . . . . : 10.20.20.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{8C7FD320-1640-4A93-8FAF-E6FE377EA0D9}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user1>ping 10.20.20.5

Pinging 10.20.20.5 with 32 bytes of data:
Reply from 10.20.20.5: bytes=32 time=20ms TTL=128
Reply from 10.20.20.5: bytes=32 time=9ms TTL=128
Reply from 10.20.20.5: bytes=32 time=6ms TTL=128
Reply from 10.20.20.5: bytes=32 time=18ms TTL=128

Ping statistics for 10.20.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 20ms, Average = 13ms

C:\Users\user1>ping 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Reply from 10.20.20.33: Destination host unreachable.
Reply from 10.20.20.33: Destination host unreachable.
Reply from 10.20.20.33: Destination host unreachable.
Reply from 10.20.20.33: Destination host unreachable.

Ping statistics for 10.20.20.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\user1>ping 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.31: bytes=32 time=51ms TTL=128
Reply from 10.20.20.31: bytes=32 time=18ms TTL=128
Reply from 10.20.20.31: bytes=32 time=10ms TTL=128
Reply from 10.20.20.31: bytes=32 time=26ms TTL=128

Ping statistics for 10.20.20.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 51ms, Average = 26ms

C:\Users\user1>
```

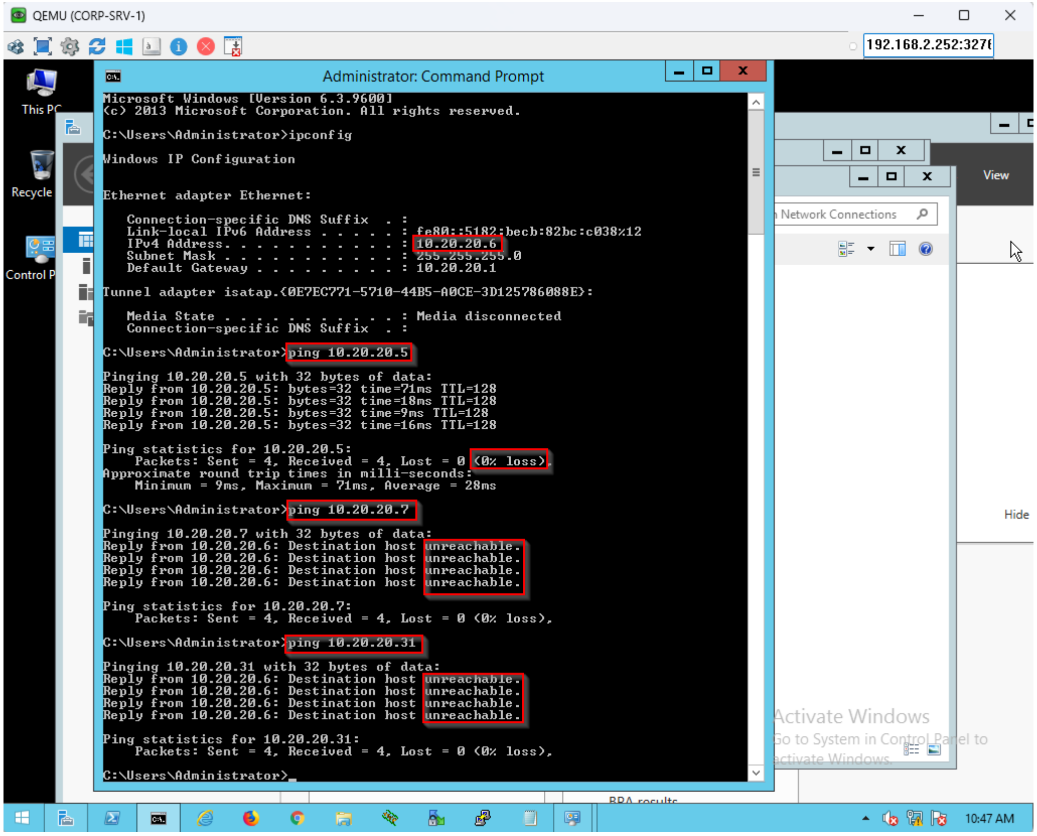
```
MGMT-PC1
user1
Windows 7
Service Pack 1
8/17/2025 3:47 AM
IP Address:     10.20.20.33
Subnet:         255.255.255.0
```

In our second test, we see that the jump server can reach the PCs and both corporate servers.



```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::750e:3b78:eda3:ad77%12
   IPv4 Address. . . . . . . . . . . : 10.20.20.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.20.1

Tunnel adapter isatap.{0E7EC771-5710-44B5-A0CE-3D125786088E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>ping 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Reply from 10.20.20.6: bytes=32 time=84ms TTL=128
Reply from 10.20.20.6: bytes=32 time=14ms TTL=128
Reply from 10.20.20.6: bytes=32 time=14ms TTL=128
Reply from 10.20.20.6: bytes=32 time=13ms TTL=128

Ping statistics for 10.20.20.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 84ms, Average = 31ms

C:\Users\Administrator>ping 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Reply from 10.20.20.7: bytes=32 time=69ms TTL=128
Reply from 10.20.20.7: bytes=32 time=13ms TTL=128
Reply from 10.20.20.7: bytes=32 time=16ms TTL=128
Reply from 10.20.20.7: bytes=32 time=16ms TTL=128

Ping statistics for 10.20.20.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 69ms, Average = 28ms

C:\Users\Administrator>ping 10.20.20.33

Pinging 10.20.20.33 with 32 bytes of data:
Reply from 10.20.20.33: bytes=32 time=61ms TTL=128
Reply from 10.20.20.33: bytes=32 time=15ms TTL=128
Reply from 10.20.20.33: bytes=32 time=15ms TTL=128
Reply from 10.20.20.33: bytes=32 time=16ms TTL=128

Ping statistics for 10.20.20.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 61ms, Average = 26ms

C:\Users\Administrator>_
```

And in our third test, we see that the corporate servers can reach the jump server, but not each other or the PCs.

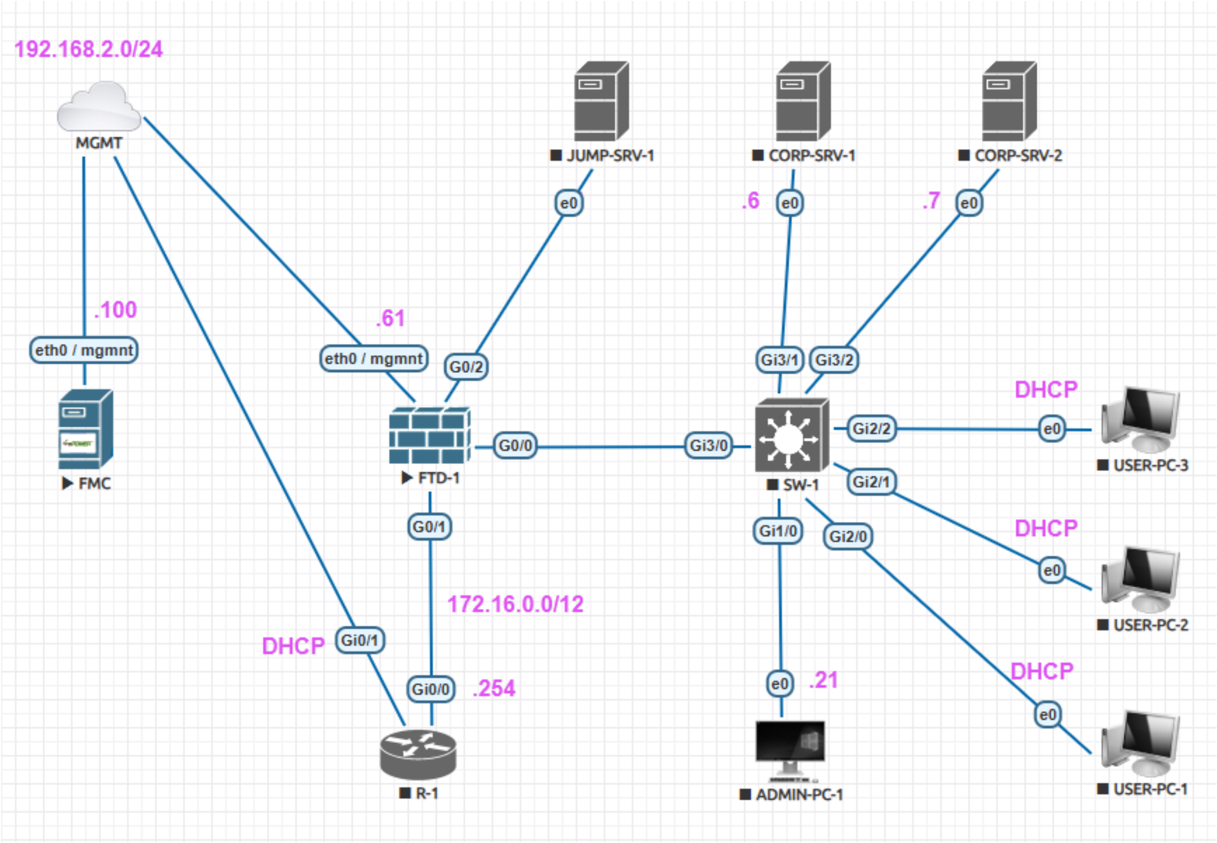


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5182:becb:82bc:c038%12
   IPv4 Address. . . . . . . . . . . : 10.20.20.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.20.1

Tunnel adapter isatap.{0E7EC771-5710-44B5-A0CE-3D125786088E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>ping 10.20.20.5

Pinging 10.20.20.5 with 32 bytes of data:
Reply from 10.20.20.5: bytes=32 time=71ms TTL=128
Reply from 10.20.20.5: bytes=32 time=18ms TTL=128
Reply from 10.20.20.5: bytes=32 time=9ms TTL=128
Reply from 10.20.20.5: bytes=32 time=16ms TTL=128

Ping statistics for 10.20.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 71ms, Average = 28ms

C:\Users\Administrator>ping 10.20.20.7

Pinging 10.20.20.7 with 32 bytes of data:
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.

Ping statistics for 10.20.20.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>ping 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.
Reply from 10.20.20.6: Destination host unreachable.

Ping statistics for 10.20.20.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>_
```

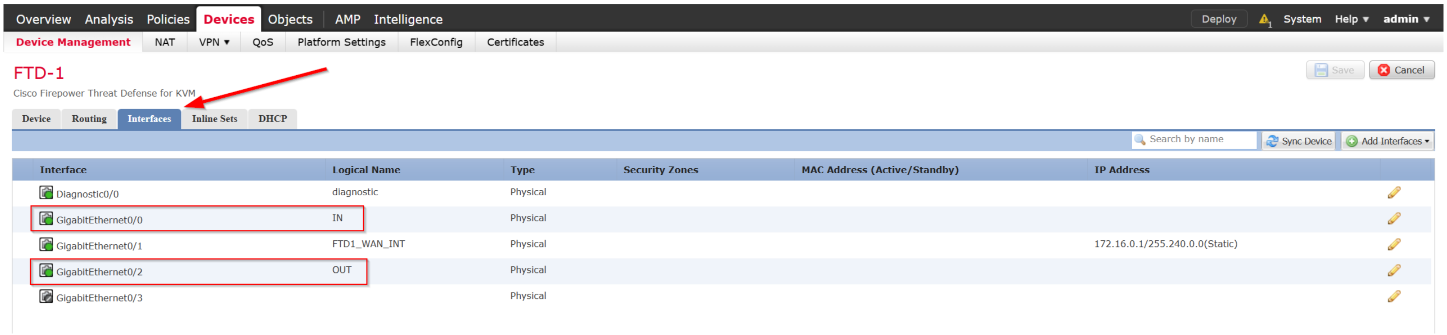
This is a job well done! Our switch shows the port association as follows. Note that the promiscuous interface Gi 3/0 shows as both isolated and community.

```
SW-1(config)#do sh vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
50      501       isolated          Gi3/0, Gi3/1, Gi3/2
50      502       community         Gi2/0, Gi2/1, Gi2/2, Gi3/0
```

As life has it, our boss comes back with a new challenge! He (rightfully) thinks that because all access to our corporate servers is provided via the jump server, we need to take extra security measures to ensure traffic from the jump server to our servers is not infected with malware. Alas! This is not something that the switch can do. For this challenge, we will need a firewall – and a special type at that, a transparent firewall. It's called "transparent" because it operates at layer 2 and is transparent to IP, making it a "bump in the wire." To place it between the jump server and other corporate servers, we need to do a bit of rewiring as well. The FTD in the current topology is configured in routed mode. In this mode, it supports inline sets, which allow the firewall to act similar to a transparent firewall while still running in routed mode. After rewiring, this is what our topology looks like.



Note that FTD-1 is now between JUMP-SRV-1 and the isolated VLAN that our corporate servers are in. Interface G0/0 of the firewall is connected to the promiscuous port Gi3/0, where the jump server was previously connected. Therefore, all traffic will go to the FTD, get examined by it, and if clean, sent to the destination. Our FTD currently has access control rules from before, which I will modify along the way when needed. Let's start with the inline set.

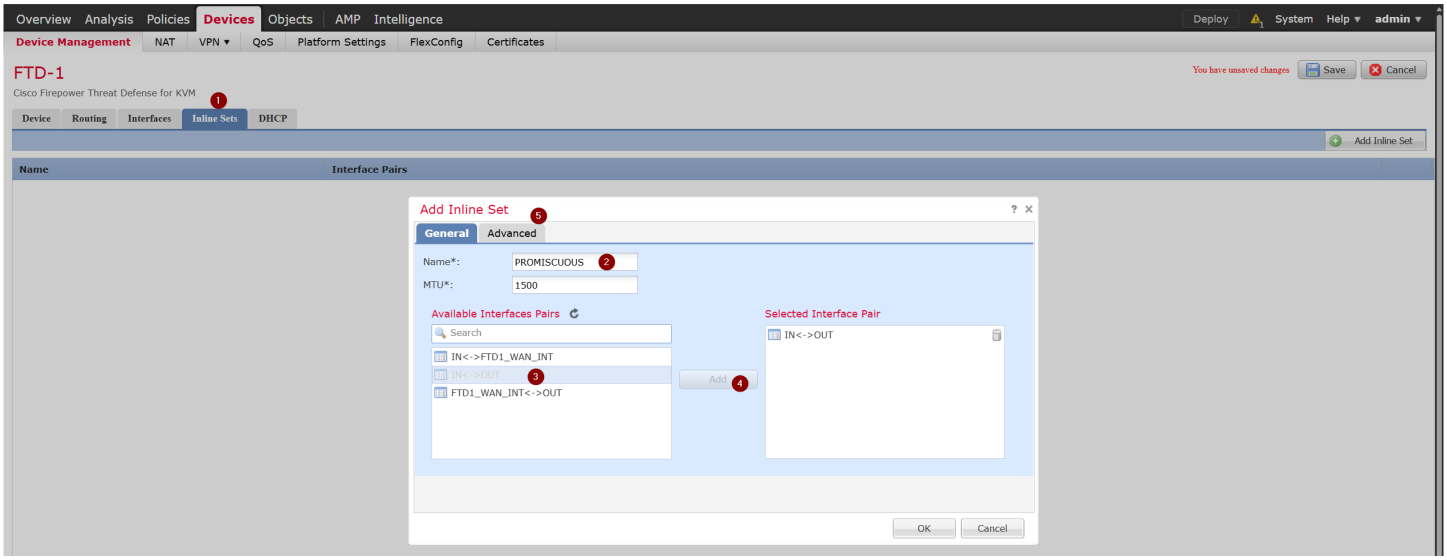


FTD-1

Cisco Firepower Threat Defense for KVM

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	IN	Physical			
GigabitEthernet0/1	FTD1_WAN_INT	Physical			172.16.0.1/255.240.0.0(Static)
GigabitEthernet0/2	OUT	Physical			
GigabitEthernet0/3		Physical			

The FMC automatically gives us a few options based on the interfaces available, as you can see below. For our scenario, the set we want is IN <-> OUT. What this does is, it essentially pairs these two interfaces such that anything that enter via one can only leave via the other – but only after inspection, and if no rules block it for any reason.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
FTD-1
Cisco Firepower Threat Defense for KVM
You have unsaved changes
Save
Cancel
Device Routing Interfaces Inline Sets DHCP
1
Add Inline Set
Name
Interface Pairs
5
General Advanced
2
3
Add
4
OK
Cancel

Add Inline Set

Name*: PROMISCUOUS

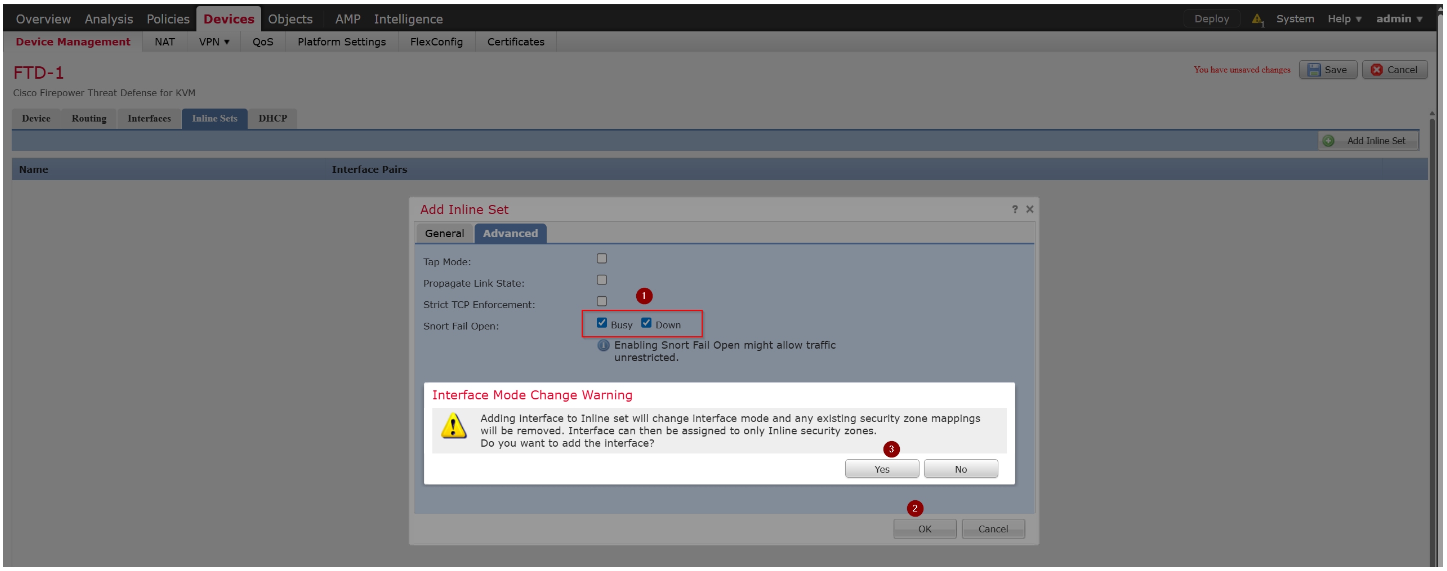
MTU*: 1500

Available Interfaces Pairs

- IN<->FTD1_WAN_INT
- IN<->OUT
- FTD1_WAN_INT<->OUT

Selected Interface Pair

- IN<->OUT


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
FTD-1
Cisco Firepower Threat Defense for KVM
You have unsaved changes
Save
Cancel
Device Routing Interfaces Inline Sets DHCP
Add Inline Set
Name
Interface Pairs
General Advanced
1
2
3
Yes
No
OK
Cancel

Add Inline Set

Tap Mode: □

Propagate Link State: □

Strict TCP Enforcement: □

Snort Fail Open: ☑ Busy ☑ Down

Enabling Snort Fail Open might allow traffic unrestricted.

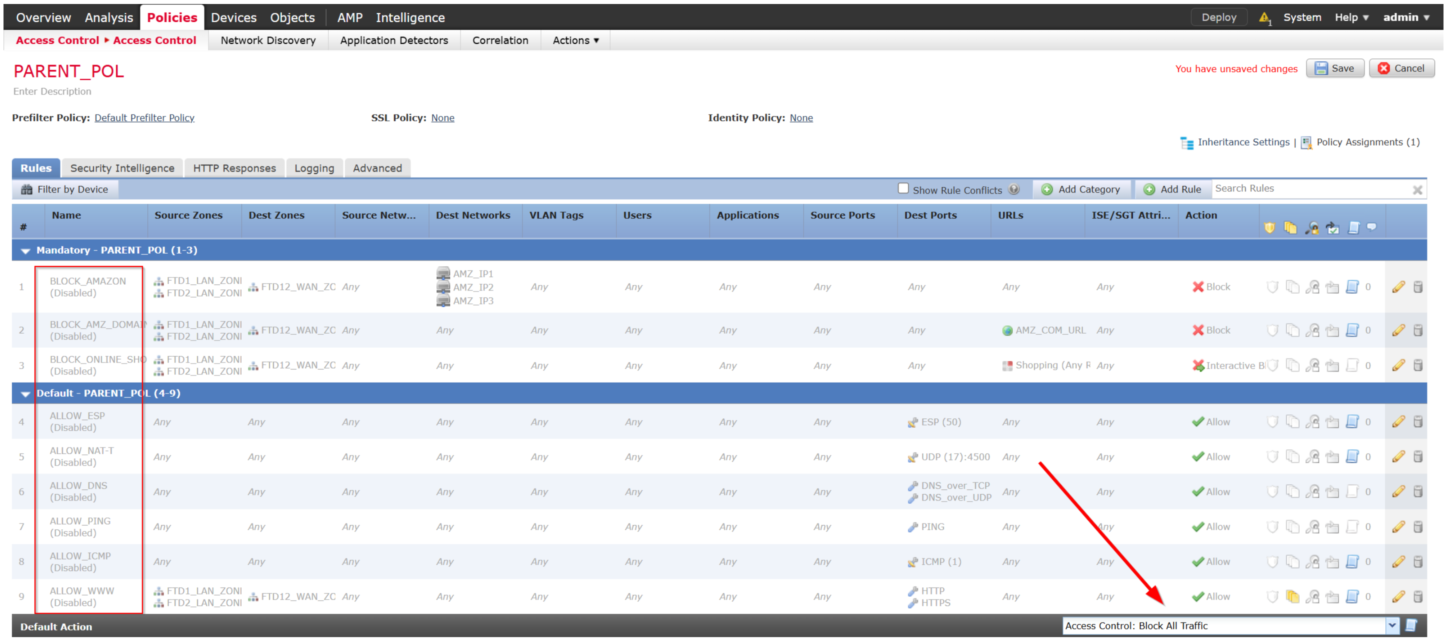
Interface Mode Change Warning

Adding interface to Inline set will change interface mode and any existing security zone mappings will be removed. Interface can then be assigned to only Inline security zones.
Do you want to add the interface?

The “Tap Mode” feature allows device to look at traffic as it passes, but the firewall will not drop anything even if it matches a rule that says drop! It changes the firewall from an Intrusion Prevention System (IPS) into an Intrusion Detection System (IDS). “Propagate Link State” controls whether the two interfaces in the inline set are aware of each other’s status. If checked and one interface goes down, the other will too, and it will come back up as soon as the first one does. “Strict TCP Enforcement” ensures that all TCP handshakes are exactly as they should be; otherwise, the traffic will be dropped. “Snort Fail Open” when busy and/or down configures the device to allow traffic through if the Snort engine is busy or unreachable. This might not sound like a good idea, but it is actually recommended to avoid random dropped traffic – especially in sensitive environments such as banks or hospitals. This is how the FTD sees our configuration:

```
> show inline-set

Inline-set PROMISCUOUS
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is on
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/0 "IN"
      Current-Status: UP
    Interface: GigabitEthernet0/2 "OUT"
      Current-Status: UP
    Bridge Group ID: 501
```

OK, let's test things. To make my life easier, I'll configure all devices with static IP addresses. I will also disable all previous rules and switch the default action to "Block All Traffic" so we get a chance to see what is going on inside our firewall.



PARENT_POL

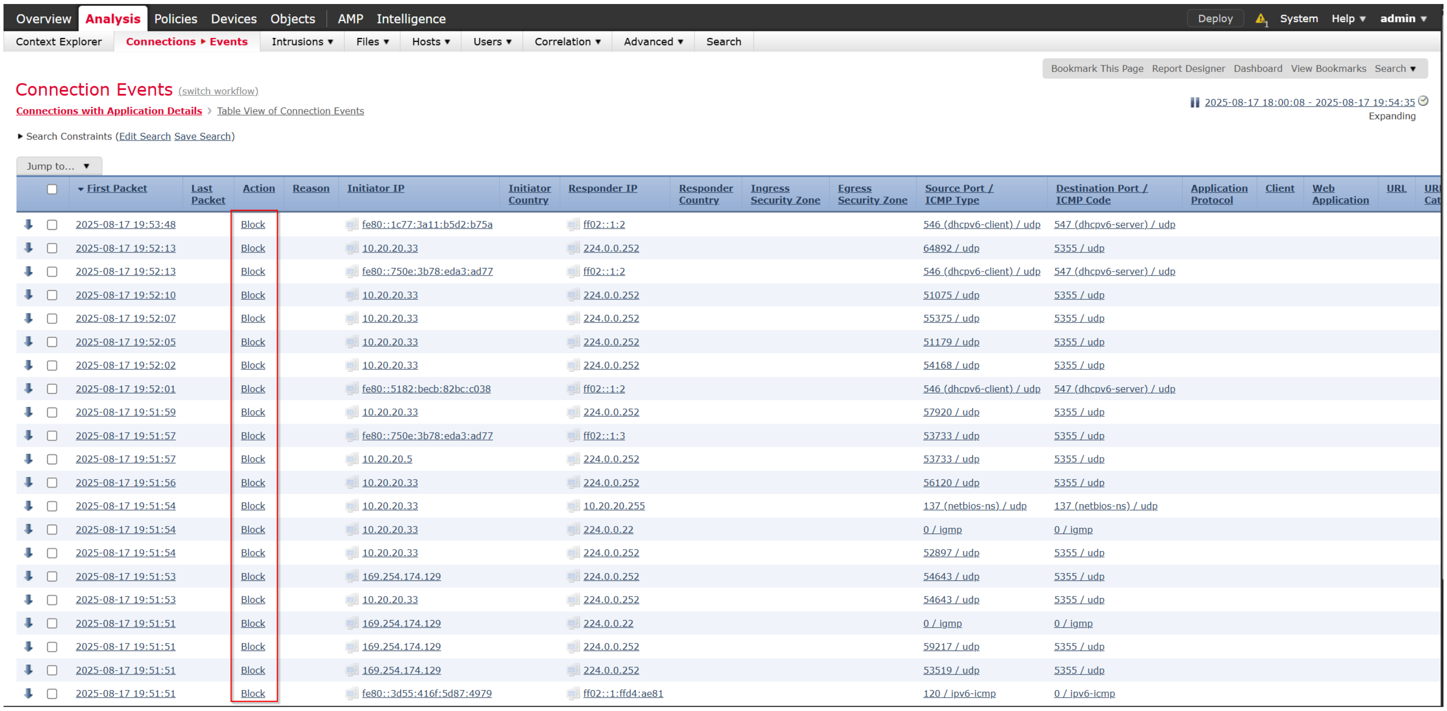
Enter Description

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	Name	Source Zones	Dest Zones	Source Netw...	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attri...	Action	
Mandatory - PARENT_POL (1-3)														
1	BLOCK_AMAZON (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12_WAN_ZC	Any	AMZ_IP1 AMZ_IP2 AMZ_IP3	Any	Any	Any	Any	Any	Any	Any	✗ Block	0
2	BLOCK_AMZ_DOMAI (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12_WAN_ZC	Any	Any	Any	Any	Any	Any	Any	AMZ_COM_URL	Any	✗ Block	0
3	BLOCK_ONLINE_SHO (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12_WAN_ZC	Any	Any	Any	Any	Any	Any	Any	Shopping (Any R	Any	✗ Interactive B	0
Default - PARENT_POL (4-9)														
4	ALLOW_ESP (Disabled)	Any	Any	Any	Any	Any	Any	Any	Any	ESP (50)	Any	Any	✓ Allow	0
5	ALLOW_NAT-T (Disabled)	Any	Any	Any	Any	Any	Any	Any	Any	UDP (17):4500	Any	Any	✓ Allow	0
6	ALLOW_DNS (Disabled)	Any	Any	Any	Any	Any	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	✓ Allow	0
7	ALLOW_PING (Disabled)	Any	Any	Any	Any	Any	Any	Any	Any	PING	Any	Any	✓ Allow	0
8	ALLOW_ICMP (Disabled)	Any	Any	Any	Any	Any	Any	Any	Any	ICMP (1)	Any	Any	✓ Allow	0
9	ALLOW_WWW (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12_WAN_ZC	Any	Any	Any	Any	Any	Any	HTTP HTTPS	Any	Any	✓ Allow	0

Default Action Access Control: Block All Traffic

After deployment, if we take a quick peek at our connection events, we already see a whole lot of blocked traffic, most of which is multicast and DHCP/LLMNR related.



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

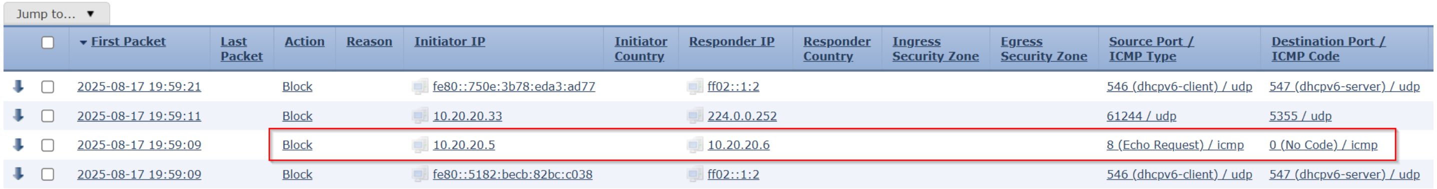
2025-08-17 18:00:08 - 2025-08-17 19:54:35

Expanding

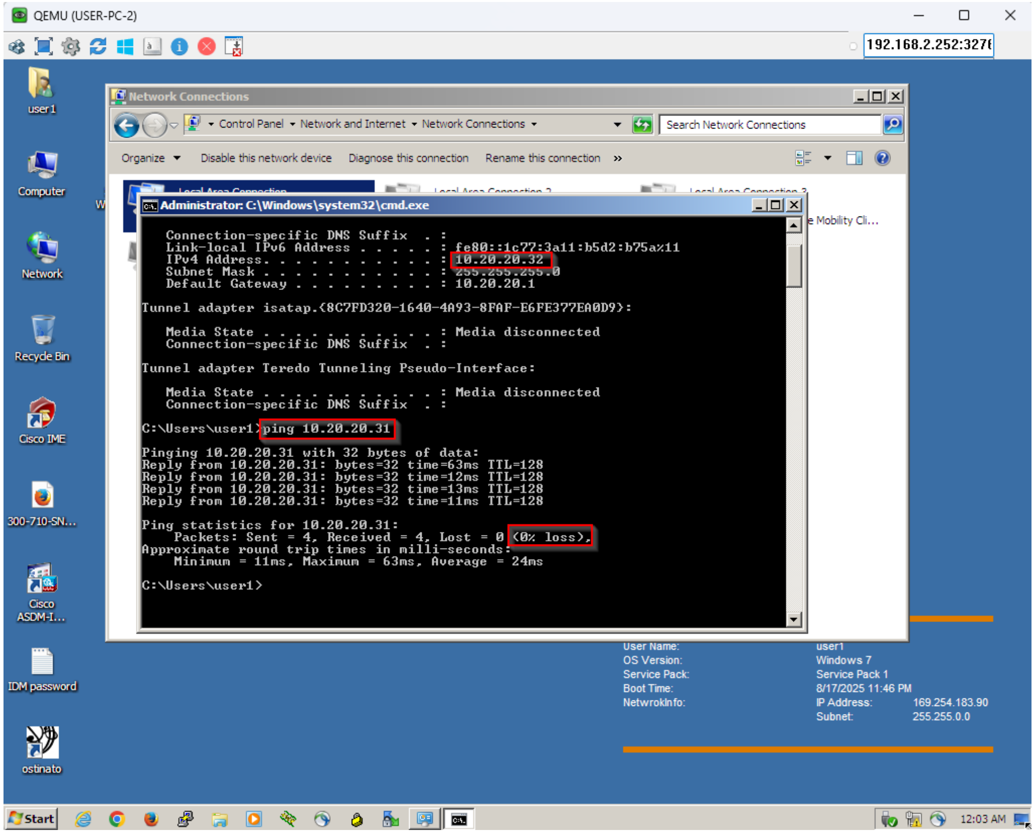
▸ Search Constraints (Edit Search Save Search)

☐	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Cat
☐	2025-08-17 19:53:48		Block		fe80::1c77:3a11:b5d2:b75a		ff02::1:2				546 (dhcpv6-client) / udp	547 (dhcpv6-server) / udp					
☐	2025-08-17 19:52:13		Block		10.20.20.33		224.0.0.252				64892 / udp	5355 / udp					
☐	2025-08-17 19:52:13		Block		fe80::750e:3b78:eda3:ad77		ff02::1:2				546 (dhcpv6-client) / udp	547 (dhcpv6-server) / udp					
☐	2025-08-17 19:52:10		Block		10.20.20.33		224.0.0.252				51075 / udp	5355 / udp					
☐	2025-08-17 19:52:07		Block		10.20.20.33		224.0.0.252				55375 / udp	5355 / udp					
☐	2025-08-17 19:52:05		Block		10.20.20.33		224.0.0.252				51179 / udp	5355 / udp					
☐	2025-08-17 19:52:02		Block		10.20.20.33		224.0.0.252				54168 / udp	5355 / udp					
☐	2025-08-17 19:52:01		Block		fe80::5182:becb:82bc:c038		ff02::1:2				546 (dhcpv6-client) / udp	547 (dhcpv6-server) / udp					
☐	2025-08-17 19:51:59		Block		10.20.20.33		224.0.0.252				57920 / udp	5355 / udp					
☐	2025-08-17 19:51:57		Block		fe80::750e:3b78:eda3:ad77		ff02::1:3				53733 / udp	5355 / udp					
☐	2025-08-17 19:51:57		Block		10.20.20.5		224.0.0.252				53733 / udp	5355 / udp					
☐	2025-08-17 19:51:56		Block		10.20.20.33		224.0.0.252				56120 / udp	5355 / udp					
☐	2025-08-17 19:51:54		Block		10.20.20.33		10.20.20.255				137 (netbios-ns) / udp	137 (netbios-ns) / udp					
☐	2025-08-17 19:51:54		Block		10.20.20.33		224.0.0.22				0 / igmp	0 / igmp					
☐	2025-08-17 19:51:54		Block		10.20.20.33		224.0.0.252				52897 / udp	5355 / udp					
☐	2025-08-17 19:51:53		Block		169.254.174.129		224.0.0.252				54643 / udp	5355 / udp					
☐	2025-08-17 19:51:53		Block		10.20.20.33		224.0.0.252				54643 / udp	5355 / udp					
☐	2025-08-17 19:51:51		Block		169.254.174.129		224.0.0.22				0 / igmp	0 / igmp					
☐	2025-08-17 19:51:51		Block		169.254.174.129		224.0.0.252				59217 / udp	5355 / udp					
☐	2025-08-17 19:51:51		Block		169.254.174.129		224.0.0.252				53519 / udp	5355 / udp					
☐	2025-08-17 19:51:51		Block		fe80::3d55:416f:5d87:4979		ff02::1:ffd4:ae81				120 / ipv6-icmp	0 / ipv6-icmp					

How about the connectivity we previously had, say from the jump server to the corporate servers or between the user devices?



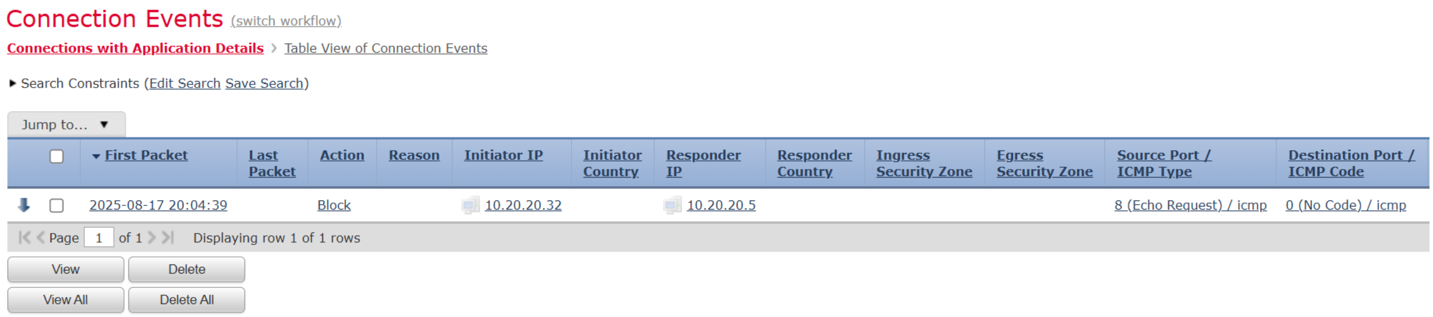
□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
□	2025-08-17 19:59:21		Block		fe80::750e:3b78:eda3:ad77		ff02::1:2				546 (dhcpv6-client) / udp	547 (dhcpv6-server) / udp
□	2025-08-17 19:59:11		Block		10.20.20.33		224.0.0.252				61244 / udp	5355 / udp
□	2025-08-17 19:59:09		Block		10.20.20.5		10.20.20.6				8 (Echo Request) / icmp	0 (No Code) / icmp
□	2025-08-17 19:59:09		Block		fe80::5182:becb:82bc:c038		ff02::1:2				546 (dhcpv6-client) / udp	547 (dhcpv6-server) / udp



```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c77:3a11:b5d2:b75a%11
   IPv4 Address. . . . . . . . . . . : 10.20.20.32
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.20.1

Tunnel adapter isatap.{8C7FD320-1640-4A93-8FAF-E6FE377EA0D9}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user1>ping 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.31: bytes=32 time=63ms TTL=128
Reply from 10.20.20.31: bytes=32 time=12ms TTL=128
Reply from 10.20.20.31: bytes=32 time=13ms TTL=128
Reply from 10.20.20.31: bytes=32 time=11ms TTL=128

Ping statistics for 10.20.20.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 63ms, Average = 24ms

C:\Users\user1>
```

User Name:	user1	
OS Version:	Windows 7	
Service Pack:	Service Pack 1	
Boot Time:	8/17/2025 11:46 PM	
NetwrokInfo:	IP Address:	169.254.183.90
	Subnet:	255.255.0.0

OK – our jump server has lost connectivity to the corporate servers, but our PCs can still reach each other. Can they get to the jump server or any corporate server, though?

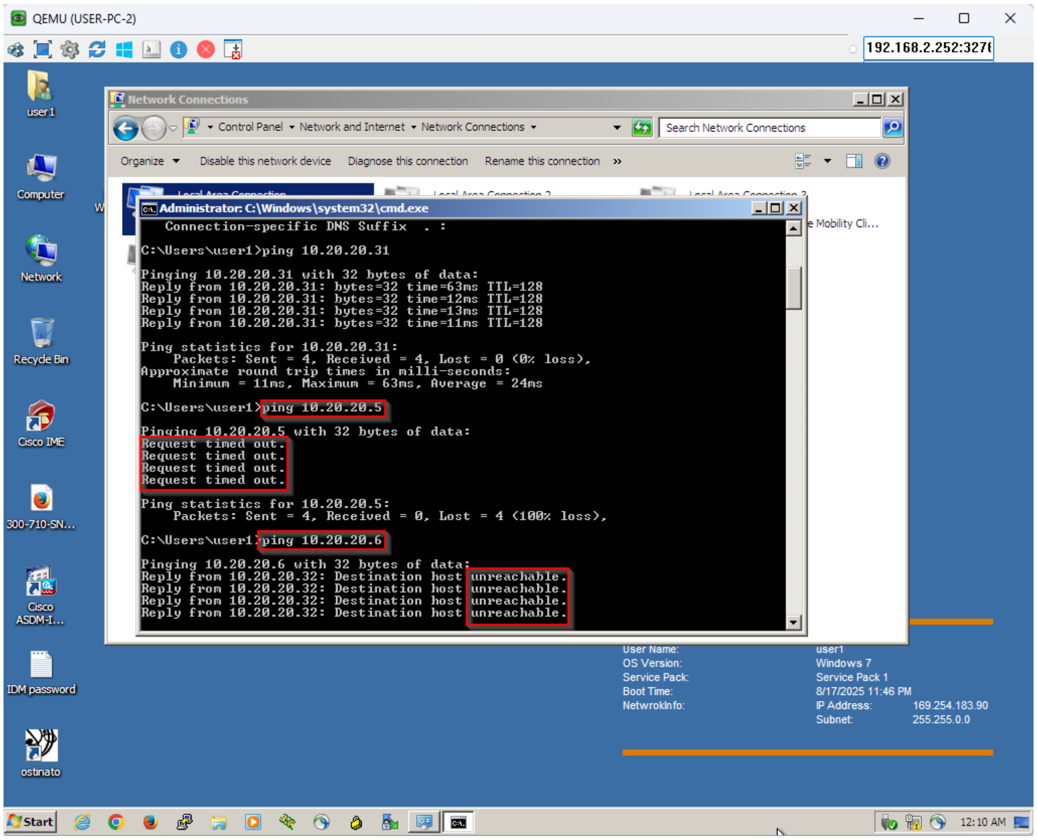

Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
□	2025-08-17 20:04:39		Block		10.20.20.32		10.20.20.5				8 (Echo Request) / icmp	0 (No Code) / icmp

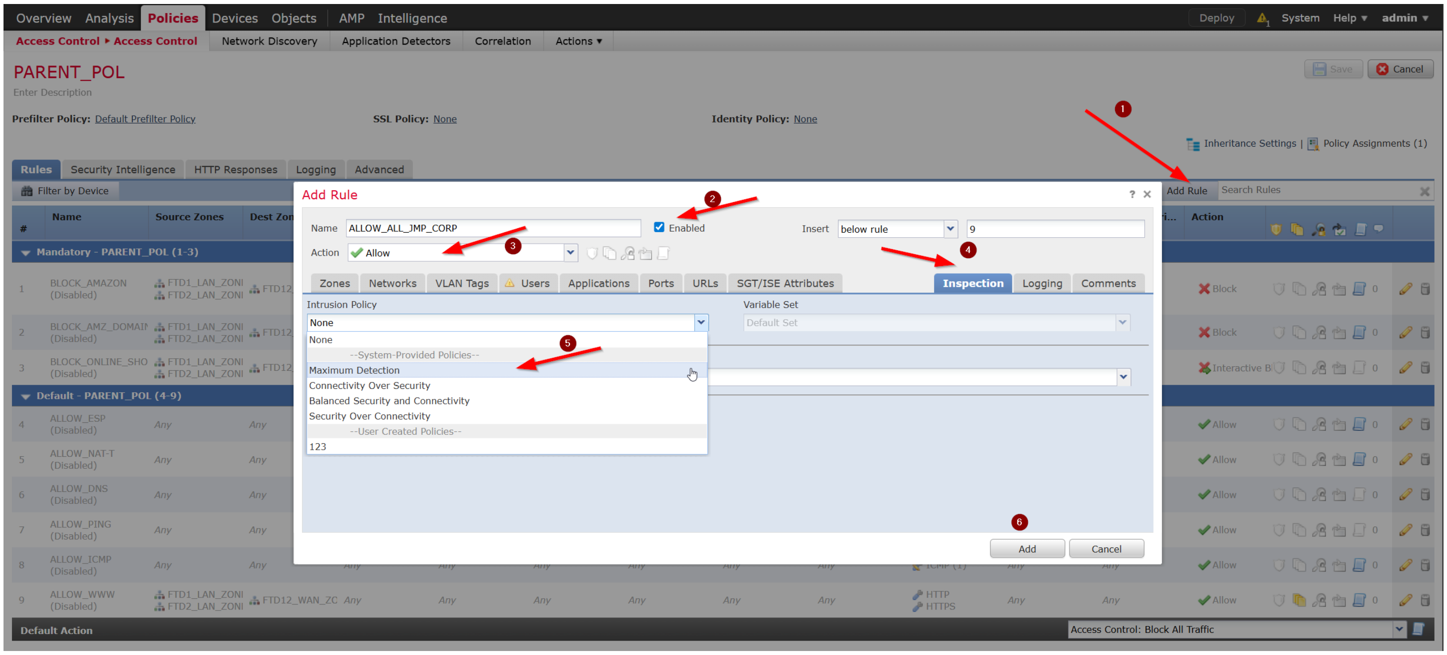
Page 1 of 1 Displaying row 1 of 1 rows



```
   Connection-specific DNS Suffix  . :

C:\Users\user1>ping 10.20.20.31

Pinging 10.20.20.31 with 32 bytes of data:
Reply from 10.20.20.31: bytes=32 time=63ms TTL=128
Reply from 10.20.20.31: bytes=32 time=12ms TTL=128
Reply from 10.20.20.31: bytes=32 time=13ms TTL=128
Reply from 10.20.20.31: bytes=32 time=11ms TTL=128

Ping statistics for 10.20.20.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 63ms, Average = 24ms

C:\Users\user1>ping 10.20.20.5

Pinging 10.20.20.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.20.20.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user1>ping 10.20.20.6

Pinging 10.20.20.6 with 32 bytes of data:
Reply from 10.20.20.32: Destination host unreachable.
Reply from 10.20.20.32: Destination host unreachable.
Reply from 10.20.20.32: Destination host unreachable.
Reply from 10.20.20.32: Destination host unreachable.
```

User Name: user1
OS Version: Windows 7
Service Pack: Service Pack 1
Boot Time: 8/17/2025 11:46 PM
Netwrokinfo: IP Address: 169.254.183.90
Subnet: 255.255.0.0

Interesting! Our firewall logs only show the attempt destined to the jump server, not the corporate servers. And the replies are different on the PC command line as well – Request timed out vs. host unreachable. The reason should be pretty obvious. Traffic sourced from the PCs and destined to the corporate servers does not go through the firewall at all. It's still the isolated VLAN configuration that is preventing access. Now, we wanted the firewall only to inspect traffic between our jump server and corporate servers. We don't want it to create any additional blocks. So, I'll go ahead and create a rule that "allows" all traffic, but inspects it for any sort of intrusion event.



PARENT_POL
Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Add Rule

Name: ALLOW_ALL_JMP_CORP   ☑ Enabled   Insert: below rule 9

Action: Allow

Intrusion Policy: None   Variable Set: Default Set

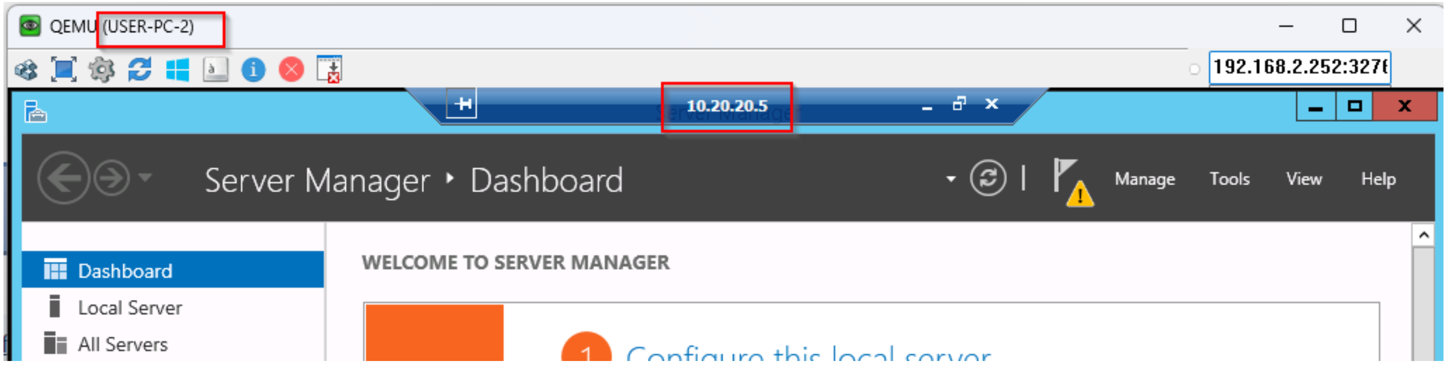
- None
- --System-Provided Policies--
- Maximum Detection
- Connectivity Over Security
- Balanced Security and Connectivity
- Security Over Connectivity
- --User Created Policies--
- 123

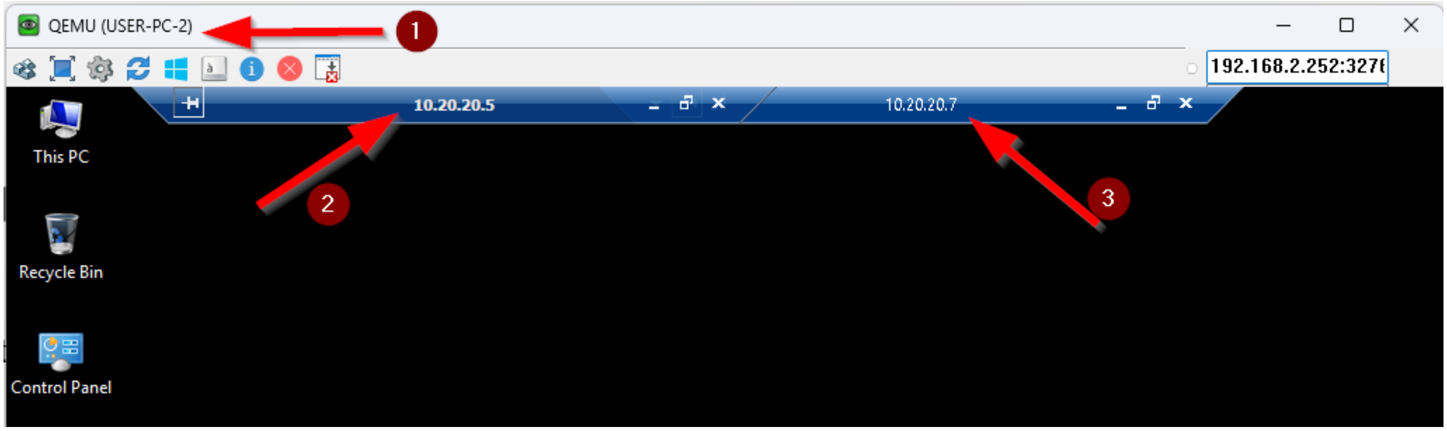
#	Name	Source Zones	Dest Zones	…	Action
	Mandatory - PARENT_POL (1-3)				
1	BLOCK_AMAZON (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12		Block
2	BLOCK_AMZ_DOMAIN (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12		Block
3	BLOCK_ONLINE_SHO (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12		Interactive B
	Default - PARENT_POL (4-9)				
4	ALLOW_ESP (Disabled)	Any	Any		Allow
5	ALLOW_NAT-T (Disabled)	Any	Any		Allow
6	ALLOW_DNS (Disabled)	Any	Any		Allow
7	ALLOW_PING (Disabled)	Any	Any		Allow
8	ALLOW_ICMP (Disabled)	Any	Any	Any Any Any Any Any ICMP (1) Any Any	Allow
9	ALLOW_WWW (Disabled)	FTD1_LAN_ZONI FTD2_LAN_ZONI	FTD12_WAN_ZC	Any Any Any Any Any Any HTTP HTTPS Any Any	Allow

Default Action: Access Control: Block All Traffic

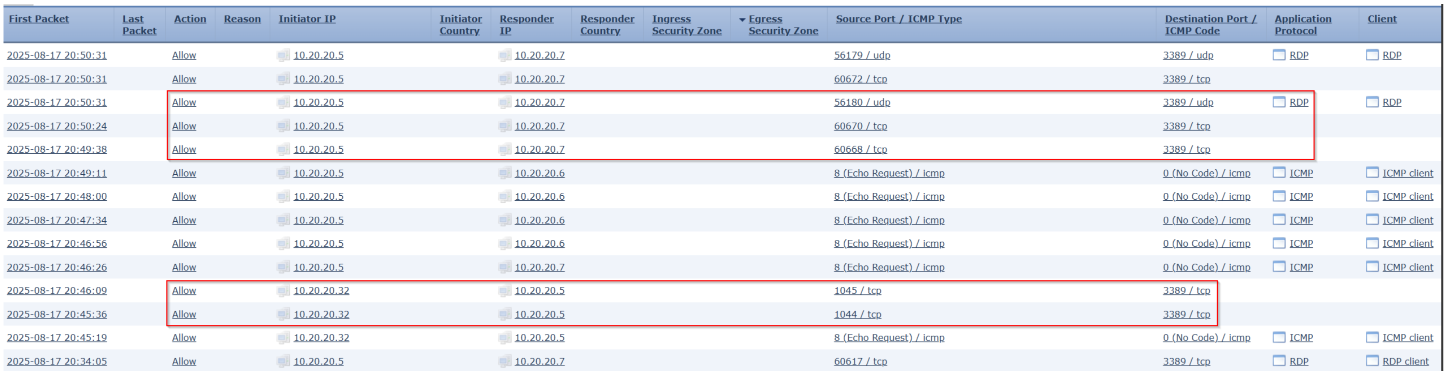
Note that I'd normally create this rule above all other rules, but since everything else has been disabled, it doesn't really matter – so, "insert below rule 9" is fine. Also, we wouldn't normally go for "Maximum Detection," as it will drop a lot of legitimate traffic as well, giving us more false positives than we want. But in this case, I am hoping it'll drop some of the traffic so I can show you the logs. "Balanced Security and Connectivity" is Cisco's recommendation.

After deployment, my pings are back to how they were supposed to be. Now let's take it up a notch. We said no access to corporate servers except via the jump server. Let's see if we can RDP into the jump server and then from there, into a corporate server.



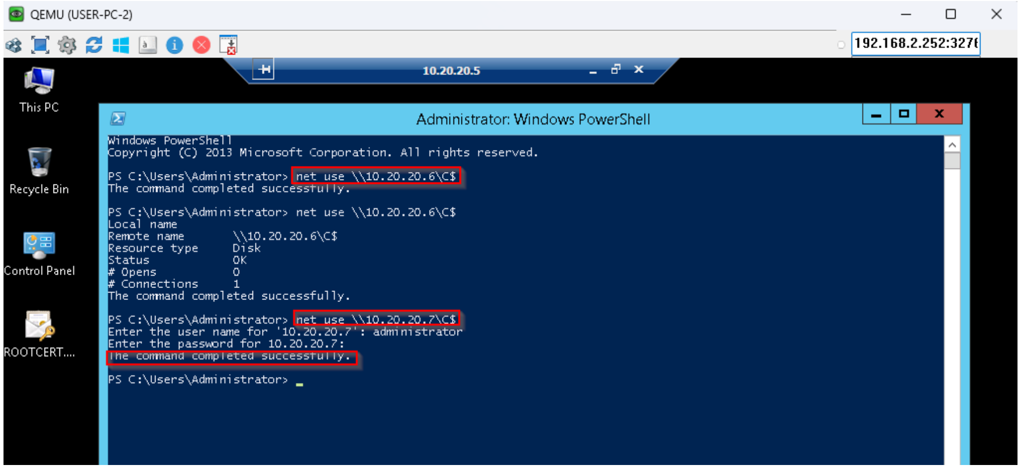


Yes, we can! Here's what the logs show.

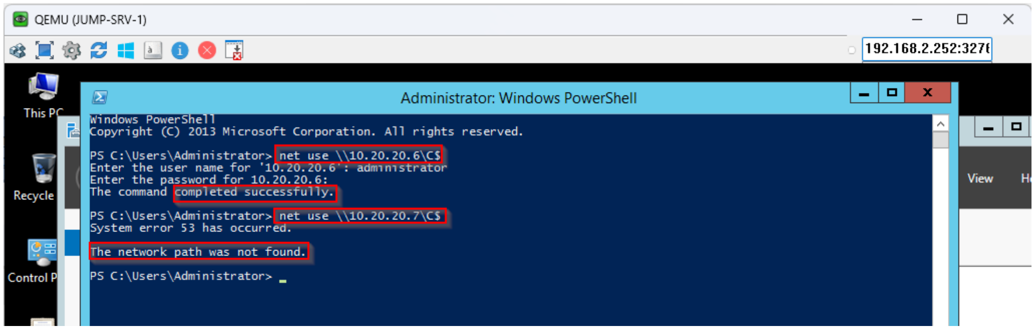


First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client
2025-08-17 20:50:31		Allow		10.20.20.5		10.20.20.7				56179 / udp	3389 / udp	RDP	RDP
2025-08-17 20:50:31		Allow		10.20.20.5		10.20.20.7				60672 / tcp	3389 / tcp		
2025-08-17 20:50:31		Allow		10.20.20.5		10.20.20.7				56180 / udp	3389 / udp	RDP	RDP
2025-08-17 20:50:24		Allow		10.20.20.5		10.20.20.7				60670 / tcp	3389 / tcp		
2025-08-17 20:49:38		Allow		10.20.20.5		10.20.20.7				60668 / tcp	3389 / tcp		
2025-08-17 20:49:11		Allow		10.20.20.5		10.20.20.6				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:48:00		Allow		10.20.20.5		10.20.20.6				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:47:34		Allow		10.20.20.5		10.20.20.6				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:46:56		Allow		10.20.20.5		10.20.20.6				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:46:26		Allow		10.20.20.5		10.20.20.7				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:46:09		Allow		10.20.20.32		10.20.20.5				1045 / tcp	3389 / tcp		
2025-08-17 20:45:36		Allow		10.20.20.32		10.20.20.5				1044 / tcp	3389 / tcp		
2025-08-17 20:45:19		Allow		10.20.20.32		10.20.20.5				8 (Echo Request) / icmp	0 (No Code) / icmp	ICMP	ICMP client
2025-08-17 20:34:05		Allow		10.20.20.5		10.20.20.7				60617 / tcp	3389 / tcp	RDP	RDP client

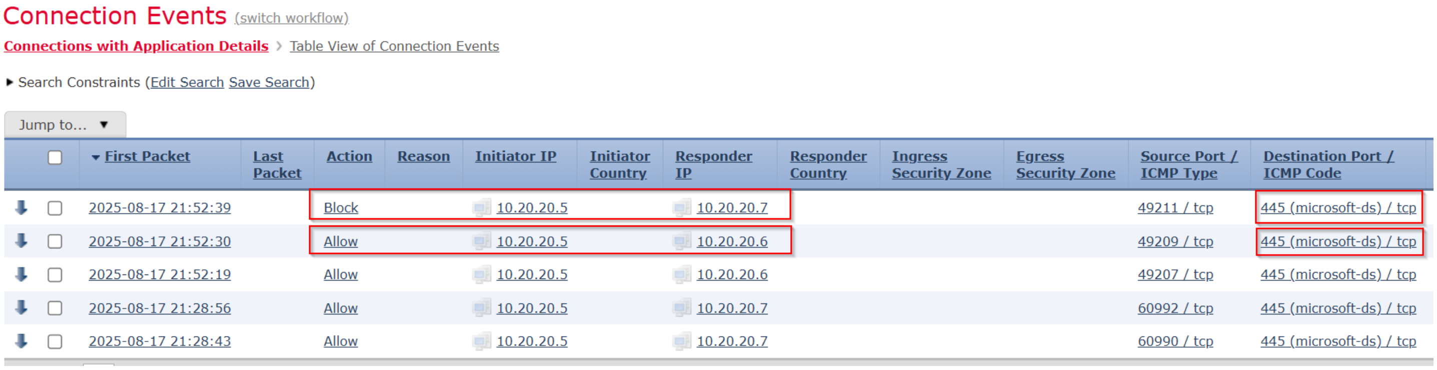
And just to give you a small taste of the power we have introduced between our jump server and corporate servers, let's create another rule that blocks SMB from the jump server to 10.20.20.7. I'll give you a before and after.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> net use \\10.20.20.6\C$
The command completed successfully.

PS C:\Users\Administrator> net use \\10.20.20.6\C$
Local name
Remote name       \\10.20.20.6\C$
Resource type     Disk
Status            OK
# Opens           0
# Connections     1
The command completed successfully.

PS C:\Users\Administrator> net use \\10.20.20.7\C$
Enter the user name for '10.20.20.7': administrator
Enter the password for 10.20.20.7:
The command completed successfully.

PS C:\Users\Administrator> _
```



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> net use \\10.20.20.6\C$
Enter the user name for '10.20.20.6': administrator
Enter the password for 10.20.20.6:
The command completed successfully.

PS C:\Users\Administrator> net use \\10.20.20.7\C$
System error 53 has occurred.

The network path was not found.

PS C:\Users\Administrator> _
```



Connection Events (switch workflow)

Connections with Application Details › Table View of Connection Events

▸ Search Constraints (Edit Search Save Search)

	□	▾ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
⬇	□	2025-08-17 21:52:39		Block		10.20.20.5		10.20.20.7				49211 / tcp	445 (microsoft-ds) / tcp
⬇	□	2025-08-17 21:52:30		Allow		10.20.20.5		10.20.20.6				49209 / tcp	445 (microsoft-ds) / tcp
⬇	□	2025-08-17 21:52:19		Allow		10.20.20.5		10.20.20.6				49207 / tcp	445 (microsoft-ds) / tcp
⬇	□	2025-08-17 21:28:56		Allow		10.20.20.5		10.20.20.7				60992 / tcp	445 (microsoft-ds) / tcp
⬇	□	2025-08-17 21:28:43		Allow		10.20.20.5		10.20.20.7				60990 / tcp	445 (microsoft-ds) / tcp

Possibilities are endless with this new solution! No matter what new challenges are thrown our way, there is probably a way to overcome them using a transparent firewall intercepting traffic.

As usual, I hope you enjoyed reading. Your feedback is most welcome 😊