Konfigurering av en Virtuell Nätverksmiljö

Jag har valt att använda Hyper-V och satt upp en virtuell Vyos Router med eth0 som extern switch, som använder min dators NIC ut till WAN som standard. Eth1 och eth2 kommunicerar lokalt, och med hjälp av NAT får dessa anslutning via eth0 och därmed internetåtkomst. Dessa implementerades genom att först skapa en virtuell router och sedan lägga till tre switchar: eth0, eth1 och eth2. Eth0 delar min dators internetanslutning, medan eth1 och eth2 är privata switchar som endast används lokalt. NAT på eth0 skyddar interna nätverk genom att dölja privata IP-adresser mot WAN, vilket minskar risken för direkta attacker från internet. Privata LAN-switchar (eth1, eth2) gör att intern trafik inte exponeras mot WAN.

Jag skapade sedan två VMer med Ubuntu ISO och använde eth1 på den ena och eth2 på den andra för att bekräfta att de kan kommunicera med varandra.

Jag har två subnät:

- Eth1: 192.168.0.1, subnet 192.168.0.0/24
- Eth2: 192.168.1.1, subnet 192.168.1.0/24

Bägge subnäten är satta på adressrange 20–50 och DHCP-leasetiden är 86 400 sekunder (1 dag). Ett /24-subnet betyder att det finns 24 nätverksbitar, vilket lämnar 32–24 = 8 bitar för hosts. 2^8 = 256 hosts, minus 2 för nät- och broadcast-adresser, ger totalt 254 möjliga enheter. Om en router används som gateway tar den 1 IP från varje subnät, vilket lämnar 253 användbara IP-adresser för övriga enheter.

Exempel: Om du har ett /29-subnet innebär det 29 stycken 1:or i binärform, dvs 32–29 = 3 bitar kvar för hosts. 2^3 = 8, minus 2 för nät- och broadcast-adress, minus 1 för router = 5 adresser för hosts. Även om våra nät nu använder endast adresserna 20–50 (30 adresser) finns det fortfarande utrymme för framtida expansion, eller för att tilldela statiska adresser upp till 253. Genom att ha ett begränsat DHCP-range och separata subnät kan man minska risken för IP-konflikter och oönskade enheter på nätverket. Detta begränsar möjligheten för obehöriga att koppla in sig på nätverket.

Firewall settings

Configure mode är förväntad för varje del, samt commit och save för att spara och skriva in inställningarna i bootfilen. Jag har valt att implementera regler på IPv4 eftersom det är det vanligaste, och planen var att blockera inkommande IPv6 om det ändå inte används på min router. Om detta ska implementeras på annan plats behöver man tänka på om man vill ha regler för IPv6 också.

Detta skapar en policy som automatiskt droppar all inkommande trafik som inte matchar några regler:

- Set firewall WAN-IN default-action drop
- set firewall ipv4 name WAN-IN rule 10 action accept
- set firewall ipv4 name WAN-IN rule 10 established
- set firewall ipv4 name WAN-IN rule 10 related

Reglerna gör att redan etablerade anslutningar inte blockeras, såsom LAN-trafik som försöker nå WAN. Relaterad trafik innebär anslutningar kopplade till en redan etablerad connection, t.ex. FTP, VPN och ping-response.

- set firewall ipv4 name WAN-IN rule 20 description “allow ssh from WAN”
- set firewall ipv4 name WAN-IN rule 20 default-action accept
- set firewall ipv4 name WAN-IN rule 20 destination port 2000
- set firewall ipv4 name WAN-IN rule 20 protocol tcp
- set firewall ipv4 name WAN-IN rule 20 log

Vi skapar sedan zoner

- set firewall zone WAN member interface eth0
- set firewall zone LAN1 member interface eth1
- set firewall zone LAN2 member interface eth2
- set firewall zone WAN from WAN firewall name WAN-IN #här allokeras zonen till reglerna WAN-IN

Anledningen till zonerna är att organisera trafikflödet baserat på typ av nätverk, vilket gör det enklare att applicera policyer och skapar en tydligare struktur som underlättar underhåll.

Vi skapar även en regel för att droppa ICMP (ping) från internet, eftersom detta kan användas för kartläggning av det interna nätverket:

Exempel:

- set firewall ipv4 name wan-in rule 30 action drop
- set firewall ipv4 name wan-in rule 30 protocol icmp #vi tillämnar samma mellan LAN1-LAN2

Jag implementerar loggning på action drop, dvs allt som skulle droppas loggas. Detta ger spårbarhet och fungerar som en säkerhetsåtgärd:

- set firewall ipv4 name wan-in rule 40 action drop
- set firewall ipv4 name wan-in rule 40 log

Outbound-trafik tillåts för LAN1 och LAN2:

- set firewall ipv4 name LAN1-TO-WAN default-action accept
- set interfaces ethernet eth1 firewall out name LAN1-TO-WAN #applicerar outbound trafik till eth1
- set interfaces ethernet eth2 firewall out name LAN2-TO-WAN #samma för ETH2
- set firewall ipv4 name LAN2-TO-WAN default-action accept

NAT

Network Address Translation (NAT) innebär att routern byter ut den privata IP-adressen från en enhet i det lokala nätverket mot routerns offentliga IP-adress när paket skickas ut till internet. Routern håller också reda på trafiken så att svaren från internet kommer tillbaka till rätt enhet i nätverket.

Exempel på port forwarding:

- set nat destination rule 45 description 'SSH port forwarding”
- set nat destination rule 45 protocol tcp
- set nat destination rule 45 destination port 2000
- set nat destination rule 45 translation address 192.168.1.50
- set nat destination rule 45 log
- set nat destination rule 45 translation port 22
  #Detta skapar en portforwarding från WAN-port 2000 till 192.168.1.50:22, vilket loggas och kan användas för underhåll på lokal nivå. SSH-nycklar kan sedan användas för säker åtkomst.

Monitoring

Vi kan övervaka med kommandon som show log och show cpu. Loggar finns på firewall-regler och andra detaljerade firewall regler med action drop och användning av DNAT. Övervakning och loggning gör det möjligt att upptäcka obehöriga försök att nå nätverket, mönster av attacker eller felkonfigurerad trafik. Detta är en viktig del av nätverks säkerheten och incidenthantering.

DHCP

När en enhet startar utan en statisk IP-adress, har den från början adressen **0.0.0.0**. Den skickar då en förfrågan om IP-adress till DHCP-servern i nätverket. Servern svarar med vilka adresser som finns tillgängliga att leasa, samt vilken adress som erbjuds till enhetens MAC-adress.

Enheten accepterar erbjudandet och bekräftar att den vill använda den tilldelade adressen. Därefter skickar servern den leasade IP-adressen tillsammans med annan nödvändig nätverksinformation, som exempelvis DNS-server och standardgateway. Nu har enheten fått en fungerande IP-adress via DHCP och kan kommunicera i nätverket.

Default route

För att enheter som inte har direkt WAN-åtkomst ska kunna nå internet via routern måste vi konfigurera en default route: set protocols static route 0.0.0.0/0 next-hop 192.168.0.1

Detta innebär att all trafik från en enhet med 0.0.0.0 som källa skickas till nästa hopp, 192.168.0.1 (LAN1-switchen). LAN1-switchen har tidigare konfigurerats så att den får internet via eth0. Detta definierar default gateway för enheter i LAN1-subnätet och säkerställer att all trafik filtreras genom routerns firewall/NAT, vilket minskar risken för oönskad exponering.

Vi kan bekräfta att routingen fungerar korrekt genom att pinga exempelvis 8.8.8.8 från enheten.

Uppsatt struktur på min router.

```
group {
    interface-group LAN {
        interface eth1
    }
    interface-group WAN {
        interface eth0
    }
}
ipv4 {
    name LAN1-FW {
        default-action accept
    }
    name LAN1-TO-LAN2 {
        default-action accept
        rule 10 {
            action drop
            description "BLOCK ICMP between LAN1 AND LAN2"
            protocol icmp
        }
    }
    name LAN1-TO-WAN {
        default-action accept
    }
    name LAN2-FW {
        default-action accept
    }
    name WAN-IN {
        default-action drop
        rule 10 {
            action accept
            state established
            state related
        }
        rule 15 {
            action accept
            destination {
                port 22
            }
            log
            protocol tcp
            source {
                address 192.168.0.104
            }
        }
        rule 20 {
            action accept
            description "Allow ssh from WAN"
:
```

```
        }
        rule 20 {
            action accept
            description "Allow ssh from WAN"
            destination {
                port 2000
            }
            protocol tcp
        }
        rule 30 {
            action drop
            description "drop ping from WAN"
            protocol icmp
        }
        rule 40 {
            action drop
            description "Log all dropped traffic"
            log
        }
    }
}
zone LAN1 {
    from LAN1 {
        firewall {
            name LAN1-TO-LAN2
        }
    }
    member {
        interface eth1
    }
}
zone LAN2 {
    member {
        interface eth2
    }
}
zone WAN {
    from WAN {
        firewall {
            name WAN-IN
        }
    }
    member {
        interface eth0
    }
}
[edit]
vyos@vyos#
```