Katowice, 01.08.2021 r.

Specyfikacja

Modernizacja zabezpieczeń teleinformatycznych poprzez wdrożenie rozwiązania firewall **pfSense** z jednoczesnym rozpoczęciem procesu migracji obecnego środowiska wirtualnego Vmware do **ProxmoxVE** (instalacja i konfiguracja pierwszego hosta wirtualizacji)

Spis treści

Cel i zakres specyfikacji

Głównym celem specyfikacji jest wdrożenie centralnego rozwiązania typu firewall ulokowanego na styku sieci VLAN funkcjonujących w ramach infrastruktury sieciowej Szkoły Policji w Katowicach. Rozwiązanie to umożliwi monitorowanie, filtrowanie ruchu i zapewni funkcjonalności brzegowego firewalla, routera oraz serwera VPN. Firewall zostanie uruchomiony w ramach nowego środowiska wirtualnego ProxmoxVE, skonfigurowanego po wyłączeniu z funkcjonowania jednego z obecnych hostów systemu wirtualizacji VMWare 6.0.

Analiza obecnej infrastruktury informatycznej

Trzon infrastrukturę serwerowej i sieciowej Szkoły Policji w Katowicach stanowią m.in.:

Serwery wirtualizacji (3 szt.) o następującej konfiguracji (najważniejsze parametry):

Prodecent, model	HP, DL360 Gen9
CPU	2x Intel E5-2630v3
RAM	128GB
Storage	Pamięć flash 8GB
Karta FC	2x HBA HP81E 8GB
System operacyjny	Vmware Vsphere ESXi 6

Macierz dyskowa o następującej konfiguracji:

Producent model	HP, MSA2040A
Dyski	24x SAS 6G 600GB
Kontrolery	2x 4-port FibreChannel Controller

Macierz została połączona redundantnie z serwerami wirtualizacji (każdy serwer jest podłączony do obu kontrolerów w macierzy). W oparciu o dostępne dyski uruchomione zostały 2 grupy dyskowe (11 dysków z poziomem ochrony RAID6). 2 dyski stanowią dyski hot-spare dla tych grup.
Na dyskach zaalokowano LUNy na potrzeby obecnie funkcjonującego środowiska wirtualnego Vmware 6.0. Bieżąca alokacja grup RAID łącznie nie przekracza 75% dostępnej przestrzeni dyskowej.

Urządzenie NAS QNAP posiadające 4 dyski zgrupowane RAID5, o wolnej do zaalokowania przestrzeni ~11TB. Możliwość użycia jedynie NFS/SMB.

Urządzenie NAS Netgear Ready NAS 314 przeznaczone do realizacji backupu środowiska Vmware Vsphere ESXi6, zaalokowane w całości na jego potrzeby. Udostępniony LUN wystawiony po iSCSI do środowiska VMWARE.

Przełączniki sieciowe Cisco Catalyst 3650 (2szt.), połączone w stos, do którego podłączono serwery wirtualizacji oraz połączenia z punktami dystrybucji sieci w budynkach szkoły. Stos przełączników stanowi centralny punkt sieci Szkoły Policji w Katowicach.

Rozwiązania docelowe adresujące problemy infrastruktury teleinformatycznej

Wymagania i zakres czynności do wykonania w ramach zadania instalacji firewalla pfSense

Celem instalacji pfSense jest zastąpienie obecnie funkcjonujących w infrastrukturze Zamawiającego routerów rozwiązaniem centralnym, pozwalających na realizację kontroli i filtrowania ruchu, jak również logowanie połączeń i aktywny monitoring sieci.

Kontrola i identyfikacja źródła ruchu (przypisanie ruchu do użytkownika sieci) jest szczególnie istotna dla sieci CSD. W tym celu w PfSense zostaną wdrożone:

- mechanizm autentykacji użytkowników sieciach CSD_SLUCHACZE, CSD_GUEST, dla sieci CSD_GUEST uruchomiony system Voucherów dostępowych.
- mechanizm umożliwiający blokowanie po adresach IP (IP Blocking) i nazwach domenowych (DNS Sinkholing) w oparciu o dostarczone zewnętrzne źródła (CERT, inne stabilne listy), jak również własne listy.
- mechanizmy umożliwiający logowanie zapytań DNS i wykluczający możliwość użycia innych DNS niż te kontrolowane przez Zamawiającego, w tym również zewnętrznych serwerów DNS over HTTPS (DoH)
- wdrożenie globalnych polityk firewall zgodnie ze szczegółowymi wymaganiami w dalszej części dokumentu.

Rozwiązanie aktywnego monitoringu zostanie wdrożone i skonfigurowany w oparciu o dodatkowy pakiet ntopng.

W ramach PFSense zostaną uruchomione również usługi: lokalny serwer NTP, Serwer TFTP, Serwer OpenVPN, Urząd Certyfikacji (OpenSSL)

Sposób instalacji pfSense

Najnowsza stabilna wersja pfSense Community Edition, zostanie zainstalowane jako maszyna wirtualna w systemie ProxmoxVE. Pfsense zostanie podłączony do sieci gospodarza w trybie popularnie nazwanym „router-on-a-stick”, poprzez jeden wirtualny interfejs sieciowy. Tagowanie i konfiguracja VLAN leży po stronie Pfsense.

Pakiety dodatkowego oprogramowania

W celu realizacji wymagań zostanie zainstalowany następujący zestaw dodatkowych pakietów z repozytorium pfSense:

1. **pfBlockerNG-devel** – narzędzie umożliwiające generowanie IPv4/IPv6 blocklist na podstawie zewnętrznych źródeł i użycie ich w regułach firewalla, Blokowanie po nazwach domenowych (DNBL) za Unbound DNS resolver. Logowanie zdarzeń.

2. **Bind –** dodatkowy serwer DNS, zainstalowany w celu możliwości wyboru forwardera na podstawie adresu źródłowego.

3. **ntopng** – zbieranie i prezentacja statystyk z działania sieci i zapisywanie do RRD. Aktywny monitoring sieci.

4. **arpwatch** – narzędzie do monitorowania aktywności i utrzymywania bazy danych par adresów adres ethernet/adres IP.

5. **Openvpn-client-export** – narzędzie do eksportu konfiguracji dla klientów OpenVPN

Konfiguracja pfSense

Czynności konfiguracyjne zostaną przeprowadzone tak aby w jak najmniejszym stopniu zakłócać bieżące funkcjonowanie sieci teleinformatycznej i będą realizowane etapami. W przypadku konieczności prace będą realizowane poza normalnymi godzinami pracy (7:30 – 15:30) Zamawiającego.

Konfiguracja centrum certyfikacji - OpenSSL CA

1. Utworzyć główny urząd certyfikacji - PFSense CA. Może być utworzony jako Self Signed lub podpisany przez funkcjonujące u CA u Zamawiającego.
2. Utworzyć dodatkowy urząd certyfikacji OpenVPN CA (typ intermediate CA) na potrzeby usługi OpenVPN (to CA będzie wystawiać certyfikaty VPN dla użytkowników Pfsense)
3. Wygenerować certyfikaty dla:
   - panelu konfiguracyjnego webowego pfSense,
   - serwera OpenVPN
   - usług Captive Portal (sieć CSD_GUEST, CSD_SLUCHACZE)
   - wygenerować certyfikaty dla użytkowników VPN wskazanych przez Zamawiającego do konfiguracji połączeń zdalnych
4. Wygenerować listy CRL

Konfiguracja PFBlockerNG

1. PfblockerNG-dev skonfigurowany w trybie „Unbound python mode”

2. Włączona funkcjonalność blokowania wildcard dla domen

3. Włączony serwer DNSBL Webserver. Zmodyfikować stronę Blocked Page (lokalizacja tekstu)

4. Włączenie logowanie zdarzeń blokowania

5. Dodanie BlockList ze stabilnych i zaufanych dostawców źródeł (np. https://hole.cert.pl/domains/domains.txt)

6. Stworzenie i dodanie własnych list w oparciu o serwer WWW Zamawiającego lub lokalne pliki systemu Pfsense.

7. Ustawienie harmonogramu aktualizacji źródeł BlockList

8. Zablokowanie użycia DNS over HTTPS (DoH) poprzez zewnętrzne Blocklisty popularnych dostawców DoH. Weryfikacja skutecznego działania blokad w popularnych przeglądarka i urządzeniach mobilnych.

Konfiguracja DNS BIND

Konfiguracja BIND jako głównego resolvera DNS dla sieci wewnętrznych. W oparciu o widoki (Views) zostanie wdrożona funkcja definiowania forwardera w zależności od źródłowego adresu IP odpytującego serwer DNS BIND.

- dla adresów IP urządzeń pracujących w VLAN CSD_GUEST, CSD_SLUCHACZE forwarderem będzie lokalny DNS Unbound, z aktywną funkcją PFBlockerNG.
- dla IP urządzeń pracujących w VLAN CWI forwarderem będzie DNS dostarczany przez KGP
- dla IP urządzeń pracujących w VLAN dla klientów Zapasowego łącza internetowego będzie DNS dostarczany przez dostawcę usług Internetu.

Konfiguracja serwera NTP

W Pfsense zostanie uruchomiony lokalny serwer NTP nasłuchujący na interfejsach sieci MGMT, SRV, CWI.

Źródłem synchronizacji czasu dla lokalnego serwera NTP będzie grupa zewnętrznych serwerów NTP. Ruch do zewnętrznych serwerów NTP przepuszczony będzie poprzez Zapasowe łącze internetowe (poprzez sieci CWI/CSD nie ma możliwości połączenia z zewnętrznymi serwerami na porcie NTP)

Konfiguracja serwera TFTP

W Pfsense zostanie uruchomiony serwer TFTP nasłuchujący na interfejsie sieci MGMT. Serwer będzie wykorzystywany do aktualizacji Firmware urządzeń sieciowych. Zostanie wdrożona polityka FW dopuszczająca tylko wybraną grupę urządzeń.

Konfiguracja usługi OpenVPN

OpenVPN zostanie uruchomiony na interfesie localhost. W celu dostępu z sieci Internet zostanie stworzona odpowiednia reguła NAT Port-forward.

Parametry serwera OpenVPN

Interface: localhost

Protocol/Port: UDP4 / 1194 (TUN)

Tunnel Network: 172.16.0.0/24

Mode: Remote Access (SSL/TLS + User Auth)

Data Ciphers: AES-256-GCM, AES-256-CBC

Digest: SHA256

D-H Params: 4096 bits

Cały ruch klienta musi być przekazywany przez tunel.

Uwaga: OpenVPN musi zostać tak skonfigurowany by serwer przypisywał zawsze ten sam adres IP dla konkretnego użytkownika VPN.

Konfiguracja Captive Portal

Funkcja portalu uwierzytelnienia zostanie skonfigurowana i uruchomiona dla sieci interfejsów VLAN : CSD_SLUCHACZE, CSD_GUEST. Źródłem autentykacji dla portalu będzie lokalna baza użytkowników PFSense.

Dodatkowo sieć CSD_GUEST musi umożliwić użycie czasowych Vaucherów na dostęp do Internetu (testowo zostaną wygenerowane vouchery w celu sprawdzenia tej funkcjonalności).

Strona portalu uwierzytelnienia zostanie zamieniona wersją zmodyfikowaną zawierającą:

- logo Zamawiającego
- odnośnik do „Regulaminu korzystania z sieci CSD” (regulamin w pliku PDF dostarczonym przez Zamawiającego)
- odnośnik do „paczki z certyfikatami dla SSLProxy” (dostarczony przez Zamawiającego plik ZIP)
- odnośnik do „Instrukcji wgrywania certyfikatów” (plik PDF)
- zapewniać responsywność (poprawność wyświetlania na różnych urządzeniach – komputer, tablet, telefon)

Uwaga: Wszystkie pliki do których kieruje muszą zostać zauploadowane do pfSense.

Przygotowana zmieniona storna uwierzytelnienia Captive Portal zostanie przetłumaczona na język polski.

Konfiguracja interfejsów VLAN i serwera DHCP

1. Dodanie wszystkich interfejsów VLAN (zewnętrznych, wewnętrzne) wykorzystywanych przez obecnie funkcjonujące w infrastrukturze Zamawiającego routery (CWI, CSD, router do łącza zapasowego).

2. Skojarzenie z wewnętrznymi interfejsami pfSense oraz konfiguracja adresacji w ramach dodanych interfejsów zgodnie z informacjami zawartymi w punkcie „Analiza obecnej infrastruktury informatycznej" Zamawiającego.

3. Konfiguracja **serwera DHCP** dla utworzonych interfejsów. Tam gdzie nie jest to wymagane ustawić zakresy przydzielanych adresów (range).

W przypadku statycznych rezerwacji DHCP, które są wprowadzone do obecnie funkcjonujących serwerów DHCP, należy wpisy te przenieść do konfiguracji pakietu DHCP w pfSense (łącznie jest to ok. **570 stacji roboczych i urządzeń** do przeniesienia). Uwaga: W przypadku rezerwacji koniecznie zaznaczyć opcję tworzenia **statycznych wpisów ARP**

4. Dla poszczególnych interfejsów ustawić właściwy adres serwer DNS, adres serwer NTP (dla tych interfejsów na których jest uruchomiona i nasłuchuje usługa lokalnego serwera NTP), adres serwera WINS

Konfiguracja reguł FW

W ramach wdrożenia pfSense zostanie opracowana globalna polityka firewall.

W celu realizacji polityki tam gdzie jest to możliwe zostanie wykorzystany mechanizm aliasów umożliwiający tworzenie grup hostów, grup portów, zapewniający wysoki poziom elastyczności rozwiązania. Opracowana zostanie też nomenklatura nazewnicza dla grup hostów, grup portów itd.

Globalna polityka powinna obejmować następujące obszary:

- zostanie zdefiniowana grupa hostów stacji roboczych Administratorów służących do zarządzania i polityka dostępu obejmująca interfejsy zarządzające w sieci MGMT oraz usługi, konsole administracyjne systemów informatycznych uruchomionych w ramach sieci SERWERY.
- zostaną określone i zdefiniowane porty potrzebne do poprawnego działania usług centralnych, świadczonych przez KGP (poczta Lotus Notes, porty niezbędne do działania agentów i endpointów na stanowiskach komputerów w sieci CWI)
- zostaną skonfigurowane dodatkowe reguły firewalla zgodnie z wymaganiami pracowników Wydziału Łączności i Informatyki lub odseparowane oddzielne obszary grup hostów o odmiennych od reszty uprawnieniach (np. ściślejsza kontrola dostępu do serwerów plikowych, systemów obiegu dokumentów)

Szkolenie dla pracowników Wydziału Łączności i Informatyki

W ramach wdrażania rozwiązania zostanie przeprowadzone szkolenie dla pracowników z obsługi wdrożonego rozwiązania PfSense. Szkolenie będzie miało postać otwartą. Prace konfiguracyjne będą realizowane z pracownikami by już na tym etapie zaznajomić z podstawowymi zadaniami konfiguracyjnymi i omówić sposoby konfiguracji urządzenia. Po przeprowadzeniu szkolenia każdy uczestnik będzie mógł sprawnie:

- dodawać i konfigurować nowe interfejsy VLAN

- konfigurować serwer DHCP, dodawać nowe urządzenia i tworzyć statyczne rezerwacji
- kreować bieżącą politykę firewall, tworzyć aliasy hostów i portów, dawać dostęp wybranej grupie hostów do wybranych usług.
- analizować logi urządzenia w zakresie logów Firewall, analizowania raportów z rozwiązania PFBlockerng-devel
- tworzyć użytkowników Captive Portal i generować czasowe Vouchery dla użytkowników sieci CSD_GUEST
- weryfikować stan usług uruchomionych na urządzenia
- używać wbudowanych w Pfsense narzędzi diagnostycznych dostępnych z GUI i konsoli

Szkolenie będzie prowadzone aż do wyczerpania tematyki związanej z funkcjonowaniem pfSense i pełnego zrozumienia przedstawionej tematyki przez biorących udział w szkoleniu. Szkolenie nie będzie krótsze niż 3h.

Podsumowanie zadania

Możliwości wdrożonego rozwiązania pfSense:

- rozwiązanie zarządzane i konfigurowane w całości poprzez panel webowy

- centralne zarządzanie i monitorowanie sieci

- logowanie połączeń

- multi gateway router, funkcja NAT

- Server OpenVPN

- Server NTP

- Server TFTP

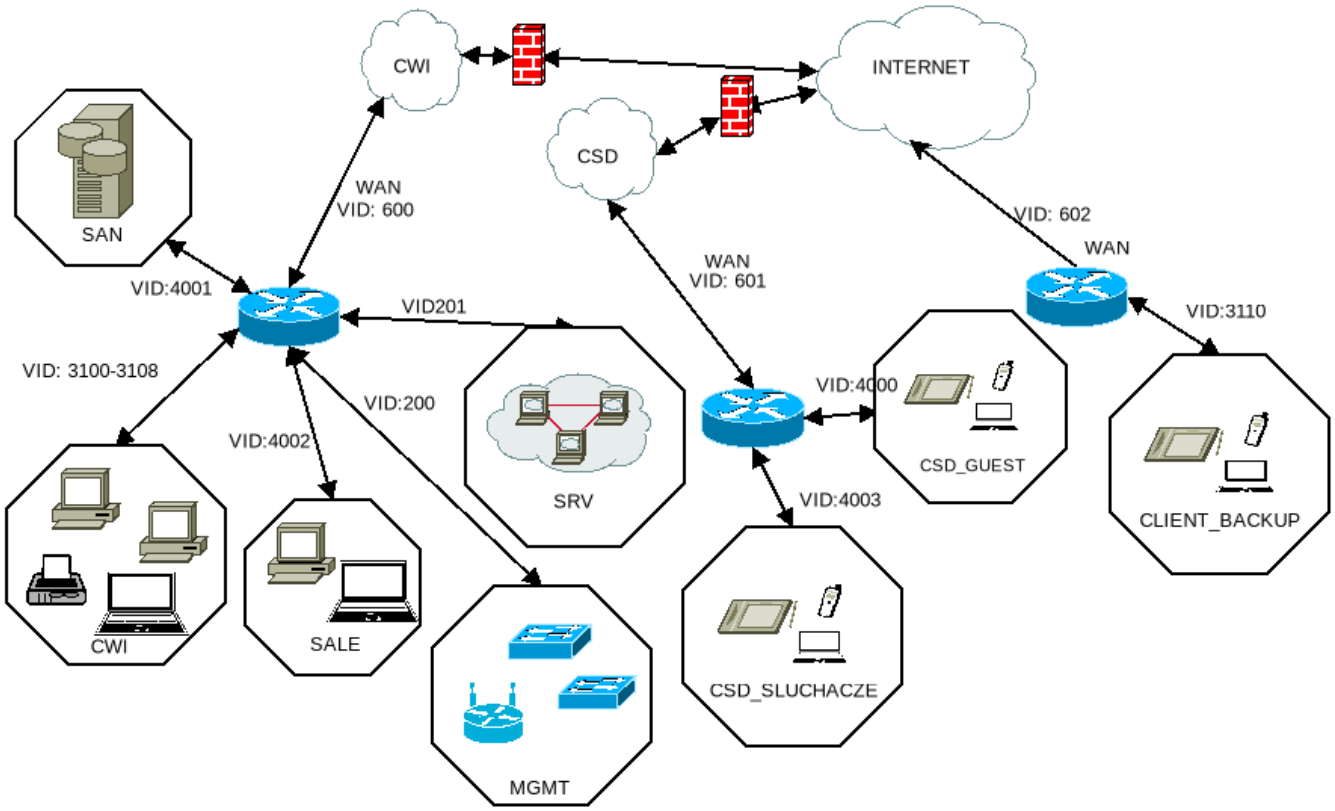
- Server DNS

- DNS Blocker(DNBL), IP Blocker (BlockList)

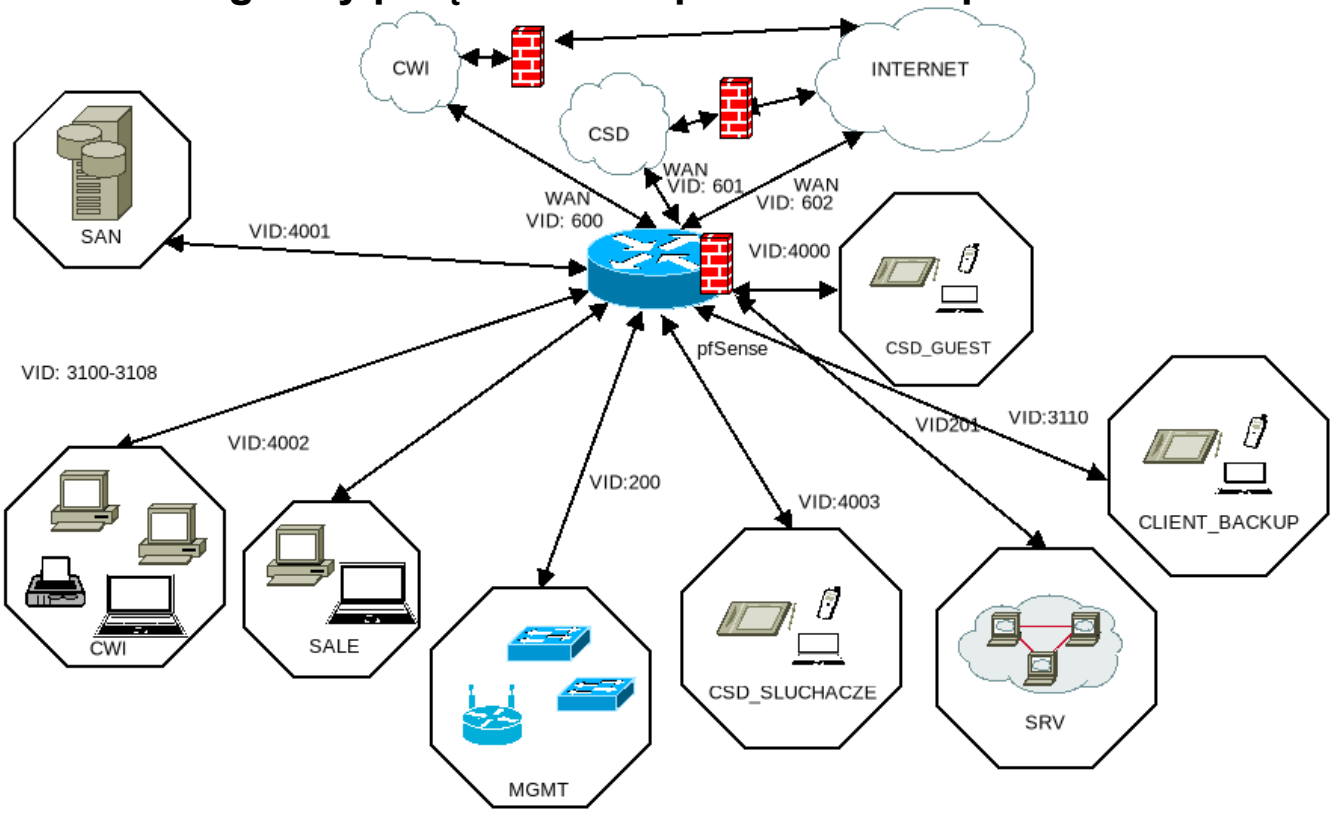
- Zaawansowany IP Firewall

- Możliwość kształtowanie ruchu Traffic-shaping

Schemat logiczny połączeń sieci przed wdrożeniem pfSense



Schemat logiczny połączeń sieci po wdrożeniu pfSense



System wirtualizacji ProxmoxVE

Wymagania i zakres czynności do wykonania w ramach zadania instalacji serwera wirtualizacji ProxmoxVE

Celem instalacji jest rozpoczęcie przez Zamawiającego procesu migracji maszyn wirtualnych z rozwiązania komercyjnego VMWARE 6.0, które utraciło już wsparcie dostawcy do rozwiązania otwartego ProxmoxVE.

Środowisko ProxmoxVE zostanie zainstalowane na jednym z obecnych hostów wirtualizacji VMWARE. Zamawiający zadba o wcześniejsze przygotowania serwera fizycznego do instalacji ProxmoxVE (przeniesienie VM na pozostałe nody klastra VMWARE, wyłączenie node z użycia).

Typ hosta: Węzeł samodzielny - nie zdefiniowano klastra

Konfiguracja sieci na hoście wirtualizacji ProxmoxVE

W ramach konfiguracji sieci zostanie wdrożone rozwiązanie openvswitch, o następującej konfiguracji:

- dostępne w serwerze 4 fizyczne interfejsy sieciowe 1G zostaną zagregowane w openvswitch (LACP balance-tcp) po odpowiedniej konfiguracji stosu przełączników Cisco.
- zostanie utworzony vbr0 na potrzeby maszyn wirtualnych
- zostaną utrzworzone następujące porty ovswitch i skonfigurowane interfejsy:

  Interfejs zarządzający (MGMT vid:200)

  Intefejs sieci SAN (SAN vid:4001)

Nazwa domenowa hosta: hpv03.ad.spkatowice.policja.gov.pl

Konfiguracja zasobów NFS

1. Wyeksportować katalogi po NFS na urządzeniu QNAP NAS na potrzeby kopii maszyn wirtualnych z środowiska Proxmox:

- backup-proxmox-daily (kopie dzienne)
- backup-proxmox-weekly (kopie tygodniowe, realizowane w soboty)
- backup-proxmox-monthly (kopie miesięczne)
- ISO (zasób na obrazy płyt ISO)

Uprawnienia do zapisu dla: hpv03, hpv02, hpv01

2. Podłączyć zasoby NFS do hosta.

3. Ustawić retencję dla każdego z zasobu podłączonego po NFS.

4. Ustawić harmonogramy backupów

Konfiguracja datastore dla maszyn wirtualnych

1. Wystawić na macierzy LUN o wystarczających rozmiarach na instalację pfSense. Dodać uprawnienia do LUN dla kart HBA zainstalowanych w hoście.

2. W hoście znajdują się 2 karty HBA, więc mamy 2 dostępne ścieżki do wystawionego LUN. W celu zachowania redundancji połączeń z macierzą zostanie wdrożony i poprawnie skonfigurowany **multipathd**

3. Na urządzeniu device mapper (DM) utworzonym przez multipath zostanie uruchomiony datastore dla VM, wykorzystując do tego celu menedżera dysków loginczych (LVM2). Nazwa grupy woluminów (VG): proxmox-datastore01. Datastore zostanie skonfigurowany w środowisku ProxmoxVE.

4. W ramach kluczowych punktów szkolenia, Wykonawca zaprezentuje jak wykonać w locie powiększenie rozmiaru uruchomionego datastore.

Przygotowanie maszyny wirtualnej VM pfsense

1. Utworzyć i przygotować konfigurację maszyny wirtualnej pod instalację pfSense

2. Interfejs sieciowy podłączony do vmbr01. Tagowanie VLAN 802.1q leży po stronie pfSense.

3. Umieścić obraz ISO z instalatorem pfSense w repozytorium ISO.

Szkolenie dla pracowników Wydziału Łączności i Informatyki

W ramach wdrażania rozwiązania zostanie przeprowadzone szkolenie dla pracowników z obsługi wdrożonego rozwiązania ProxmoxVE. Szkolenie będzie miało postać otwartą. Prace konfiguracyjne będą realizowane z pracownikami by już na tym etapie zaznajomić z podstawowymi zadaniami konfiguracyjnymi i omówić sposoby konfiguracji środowiska. Po przeprowadzeniu szkolenia każdy uczestnik będzie mógł sprawnie:

- dodawać i konfigurować nowe maszyny wirtualne (VM) w środowisku Proxmox
- wykonywać i odtwarzać kopie zapasowe całych maszyn wirtualnych (vzdump)
- konfigurować i modyfikować harmonogramy wykonywania kopii zapasowych
- powiększać dyski sieciowe VM bez zatrzymywania usług i wyłączenia VM
- powiększać datastore dla maszyn wirtualnych bez konieczności restartu hosta wirtualizacji

Szkolenie będzie prowadzone aż do wyczerpania tematyki związanej z funkcjonowaniem środowiska backupu i pełnego zrozumienia przedstawionej tematyki przez biorących udział w szkoleniu. Szkolenie nie będzie krótsze niż 3h.